Bezpečnost peer to peer aplikací

Bakalářská práce

Jiří Vaňásek

Vedoucí bakalářské práce:

Ing. Ladislav Beránek, CSc., MBA.

Jihočeská univerzita v Českých Budějovicích

Pedagogická fakulta

Katedra

2010

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval/-a samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platnémznění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách.

V Českých Budějovicích dne

Anotace

Práce se zabývá bezpečností peer to peer aplikací, používané hlavně pro sdílení souborů. Tyto aplikace jsou v současné době hodně používané a proto je důležité minimalizovat riziko při používání těchto aplikací. Součástí práce je provedení průzkumu používání peer to peer aplikací v podnicích. Další část je věnována bezpečnostnímu skenování těchto aplikací, popsání odhalených chyb a jejich odstranění.

Abstract

This bachelor thesis deals with security of P2P applications, that are mainly used for file sharing. It is very important to minimalise the hazard of using these applications, bacause they are being used a lot today. One part of the thesis is a survey of using P2P applications in corporations. The next part is devoted to security scanning of these applications, describing found errors and their elimiation.

Poděkování

Rád bych poděkoval vedoucímu mé bakalářské práce panu Ing. Ladislavu Beránkovi CSc., MBA. za jeho trpělivost a cenné rady. Dále bych chtěl poděkovat Michalu Zemanovi za poskytnutí pomoci a základních informací o bezpečnostním scanneru Nessus. A na závěr bych rád poděkoval všem respondentům, kteří se zúčastnili průzkumu používání a rizik peer to peer aplikací v podnicích.

Obsah

1 Úvod

Tato práce se zabývá problematikou týkající se bezpečností peer to peer aplikací. Je zaměřena především na aplikace zaměřené pro sdílení souborů jako jsou například BitTorrent, DirectConnect, Vaza a další. V současnosti jsou tyto aplikace velmi rozšířené a proto je žádoucí co nejvíce minimalizovat rizika způsobené používáním těchto aplikací.

První část práce je věnovaná teorii. Dozvíme se zde něco o historii peer to peer sítí, přenosu dat, definicích peer to peer sítí a jejich využití. Větší část teorie se zabývá bezpečnostními otázkami spojené s používáním peer to peer aplikací. Jsou zde popsána bezpečnostní rizika od zavlečené škodlivého softwaru až po DoS útoky.

Praktická část obsahuje bezpečností skenování testovaných aplikací, popis bezpečnostních chyb a jejich možné odstranění. Aplikace byly testovány na doma vytvořené síti a na různých operačních systémech od Windows2000, přes Windows XP, Windows Vista až po Windows7 a také Linux. Systémy Windows XP a Windows Vista byly navíc postupně ošetřeny nainstalováním všech service packů, vydanými společností Microsoft a po té otestovány. Aplikace byly testovány pomocí bezpečnostního scanneru Nessus. V poslední části této práce byl proveden průzkum používání a rizik peer to peer aplikací v podnicích a jeho vyhodnocení.

2 Peer to peer síťě

2.1 Historie peer to peer sítí

Technologie peer to peer je stejně stará jako sám internet, ovšem princip na kterém je technologie peer to peer založena je ještě mnohem starší. Jednou z prvních peer to peer komunikací byl tzv. "telegraf v džungli", tedy bubny rozmístěné v krajině, které sloužili k vzájemné komunikaci. Dalším komunikačním zařízením fungujícím na principu peer to peer sítí je telefon. Předchůdce dnešního internetu ARPANET[1] byl také navržen jako peer to peer síť, byl navržen tak aby fungoval i v momentě kdyby byly některé jeho části zničeny. V době vzniku ARPANETu však ještě neexistovala žádná počítačová kriminalita. Základ ARPANETu tvořily počítače na čtyřech univerzitách UCSB[2], SRI[3], UCLA[4] a University of Utah, k těmto počítačům měli přístup pouze vědci a kvalifikovaní pracovníci, proto se nikdo nijak zvlášť bezpečností na internetu nezabýval.

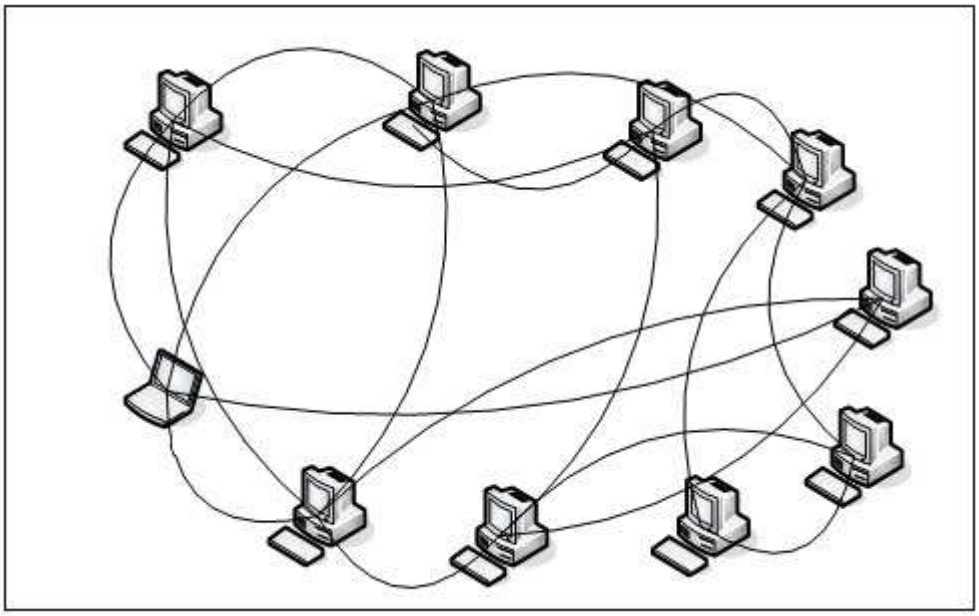
O bezpečnosti na internetu se začalo mluvit až po rozšíření internetu do komerční sféry a to počátkem devadesátých let minulého století, kdy bylo nutné zajistit potřebnou ochranu citlivých dat před vzrůstající internetovou kriminalitou. Zničehonic bylo nutné se bránit různým útokům internetových zločinců. V dalších letech se internetová síť vyvinula z původní peer to peer sítě na síť klient / server, tedy na podobu na kterou jsme zvyklí i dnes. Technologie peer to peer ovšem v současnosti používá téměř každý a to prostřednictvím aplikací určených pro komunikaci, jako je například ICQ, Skype, Miranda, QIP a nebo aplikacemi pro sdílení souborů, BitTorrent, DC++, KaZaa a mnoho dalších. Internetem se však stejně rychle s těmito

[1] Advanced Research Projects Agency Network
[2] University of California, Santa Barbara
[3] Stanford Research Institute
[4] University of California, Los Angeles

aplikacemi šíří i rady, typy a zkušenosti ostatních uživatelů o bezpečnostních dírách těchto aplikací.

2.2 Definice peer to peer sítí

Hlavní myšlenka peer to peer je založena na přímé real-time komunikaci mezi jednotlivými body v síti bez zásahu třetí strany, například serveru. Jednotlivé uzly v síti tedy pracují na stejné úrovni, každý uzel může tedy fungovat jako klient nebo server. Čistá architektura sítě peer to peer ani pojem server nezná, v praxi se s ním však můžeme velmi často setkat. Nejedná se ovšem o klasický server ale o server specializovaný, který většinou slouží k počátečnímu navázání komunikace mezi jednotlivými uzli v síti. V jiném případě se může jednat o proxy servery a to pokud spolu nemohou koncové uzly komunikovat přímo.



Obr. 1: Peer to peer síť[2].

Definice peer to peer sítí mohou být různé, ale nejčastěji se setkáváme s definicí, která je rozdělena na jednu jednoduchou a jednu složitější část.

Jednoduchá definice:

- Peer to peer je síťová architektura, ve které má každý uzel stejné schopnosti a povinnosti.

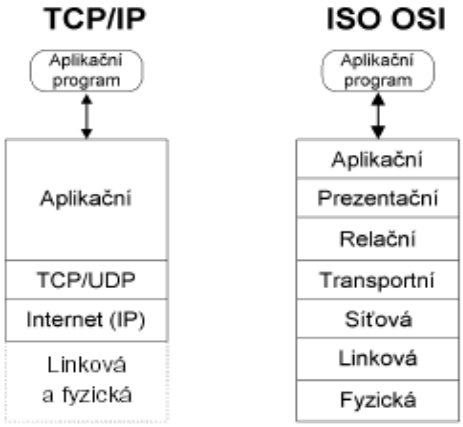
Složitá definice:

- Peer to peer síť umožňuje okamžitý přenos dat a zpráv mezi libovolnými uzli sítě.
- Každý uzel může fungovat jako klient nebo server.
- Primární obsah peer to peer sítě poskytuje každý uzel.
- Síť umožňuje kontrolu a samostatnost uzlů.
- Síť vyhovuje uzlům, které nejsou stále připojeny a které nemají pevné IP adresy.

Peer to peer aplikace musí splňovat všechny body složité definice. Pokud použijeme pouze jednoduchou definici, nebyl by například Napster peer to peer aplikací kvůli jeho centrálnímu serveru [1].

2.3 Přenos dat v peer to peer sítích

Sítě peer to peer jsou dnes nejvíce spojovány se sdílením dat. Pro přenos dat je využívaná čtvrtá vrstva podle referenčního síťového modelu ISO/OSI, který má celkem sedm vrstev. Model ISO/OSI je spíše teoretický a slouží pro porovnání různých síťových architektur a protokolů. Častěji se tedy setkáváme s modelem TCP/IP, který má vrstvy čtyři.



Obr. 2: Síťové modely[3].

Transportní vrstvě v modelu ISO/OSI odpovídají v modelu TCP/IP dva protokoly, UDP[5] a TCP[6], které zajišťují spojení mezi aplikacemi běžících na vzdálených počítačích. Protokol IP[7] má za úkol přepravovat data mezi dvěma počítači v síti, protokol TCP přepravuje pakety mezi dvěma aplikacemi, které jsou na těchto počítačích spuštěny. Protokol TCP tedy využívá k přenosu dat protokol IP. Protokol TCP tedy naváže spojení mezi těmito aplikacemi a na dobu, po kterou spolu budou tyto aplikace komunikovat vytvoří virtuální okruh, který je plně duplexní. Duplexní okruh znamená, že data mohou být nezávisle přenášeny oběma směry. Výhodou protokolu TCP je, že ošetřuje

[5] User Datagram Protocol
[6] Transport Control Protocol
[7] Internet Protocol

poškození nebo ztrátu dat, poškozená nebo dokonce ztracená data jsou vyžádána znovu a jejich správnost je ověřena kontrolním součtem. Protokol TCP si tedy neklade za cíl ochranu přenášených dat před různými útočníky, tento problém řeší například SSL protokoly.

Protokol UDP používá k přenosu dat datagramy, což je obdoba paketů. Protokol UDP nenavazuje spojení, přenos je rychlejší než u protokolu TCP, ovšem je méně spolehlivější, tudíž je používán spíše tam kde ztráta datagramu příliš nevadí. Protokol UDP jednoduše odešle datagram příjemci a dále už se nezajímá o to zda byl tento datagram úspěšně doručen. Protokol UDP je vlastně jednodušší variantou TCP protokolu [3].

2.4 Využití peer to peer sítí

Oblast ve kterých se dají peer to peer sítě využít se dá rozdělit na tři části.

- Instant messaging
- Sdílení souborů
- Disturbed computing (distribuované výpočty)

Instant massaging známý pod zkratkou IM je jednou z největších oblastí pro využití peer to peer aplikací. IM je označení pro rychlé, téměř okamžité posílání zpráv mezi uživateli. V dnešní době je samozřejmostí i přenos souborů a hlasu. IM největší mírou reprezentuje ICQ, které bylo poprvé spuštěné v listopadu roku 1996, o půl roku později mělo 800 000 aktivních uživatelů. V současné době má ICQ 40 – 50 milionů aktivních uživatelů [5]. ICQ si vytváří vlastní seznam adres, které aktualizuje v reálném čase. Tato vlastnost umožňuje ICQ obejít systém DNS[8] a zároveň je to jeden z důvodů proč je ICQ kvalifikováno jako peer to peer aplikace.

[8] Domain name system

Sdílení souborů je pravděpodobně druhá největší oblast pro využití peer to peer sítí. Fenomén stahování souborů odstartovala aplikace Napster. Tato aplikace byla vydána v roce 1999 teprve devatenáctiletým studentem Shawnem Fanningem. Napster umožňoval uživatelům mezi sebou volně šířit hudbu ve formátu MP3, obcházel tedy standardní distribuci hudby, proto také čelil řadě žalob a na příkaz soudu byla tato aplikace vypnuta. Napster však inspiroval spoustu dalších peer to peer aplikací pro sdílení souborů jako jsou například Kazza, Audiogalaxy a Gnuttela.

Třetí oblastí využití peer to peer sítě jsou tzv. distribuované výpočty. Hlavním účelem této oblasti je využití výpočetního výkonů počítačů. Dobrým příkladem distribuování výpočtů jsou rozšířené aplikace SETI@home. Aplikace SETI@home byly spuštěny v roce 1999 a již po třech měsících fungování měli jeden milión uživatelů. Hlavní funkce aplikací SETI@home byla analýza vesmírného záření za účelem hledání mimozemských civilizací. Aplikace SETI@home využívá celkem více než 5 miliónů osobních počítačů ze všech koutů planety [6].

3 Bezpečností otázky

O zabezpečení sítí se začalo hovořit až v okamžiku, kdy se internet začal šířit komerční sférou a přistup k internetu získali i běžní lidé z jejich domácích počítačů. Až do této doby byl internet využíván pouze k vědeckým účelům a všechny zúčastněné strany se o výsledky své práce dělily a pracovaly společně. Nikdo tedy neměl důvod na kohokoliv útočit, protože by tím nic nezískal. V současné době hraje zabezpečení sítí významnou roli, většina organizací a firem jsou připojené k internetu, stále více podniků využívá služeb internetu a tím dává různým internetovým útočníkům přístup do svých firemních sítí, ve kterých se mohou vyskytovat důležité informace a citlivá data. S rostoucím počtem uživatelů internetu rostou i rizika, kterým se stále více podniků a organizací vystavuje. Proto většina společností přijala preventivní bezpečnostní opatření s cílem zabezpečit jejich sítě, citlivá a tajná data. Tyto bezpečnostní opatření jsou většinou reprezentovány firewally na okrajích sítí firem. V některých případech firmy zavádějí určitou bezpečnostní politiku, která upravuje činnost jejich zaměstnanců. Velkým problémem ve spravování informační bezpečnosti je skutečnost, že bezpečnostní politiky a firewally jsou velmi často zanedbávány hned po té co jsou nainstalovány nebo zaimplementovány do systému. Výsledkem této skutečnosti je, že úroveň ochrany se stává slabší, zatímco nové hrozby informační bezpečnosti stále vznikají a vyvíjejí se.

3.1 Bezpečnostní rizika týkající se peer to peer

Bezpečnostní problémy spojené s peer to peer aplikacemi v prostředí firem jsou způsobeny několika důležitými faktory.

Prvním z těchto faktorů je, že všechny aplikace jsou určené pro kontrolované použití za firewallem. Většina peer to peer aplikací je navržena tak, aby změnila komunikační porty na porty běžně používané. Aplikace tedy

používají shodné porty, které standardně používají jiné důležité aplikace nebo pokud aplikace potřebuje, sama si hledá otevřené porty. Skutečnost, že peer to peer aplikace používají jiné porty, je o to vážnější pokud aplikace použije port 80. Port 80 je standardní port pro internetovou komunikaci – přenos WWW stránek, z tohoto důvodu musí většina firewallů tuto komunikaci přijmout, jinak by nebylo možné získat přístup k internetu z vnitřní strany firewallu. Standardním protokolem používaný pro přenos WWW stránek je protokol HTTP[9]. V tomto momentně nastává problém. Většina peer to peer aplikací používá protokol HTTP jako transportní protokol pro přenos zpráv a souborů. Pokud tedy peer to peer aplikace použije port 80 a protokol HTTP, vytvoří komunikaci podobnou běžnému přenosu WWW stránek [1].

Dalším závažným faktorem, který se týká zejména sdílení dat, je fakt že uživatel nemá nikdy stoprocentní jistotu, že jím stahovaný soubor neobsahuje žádný škodlivý software. Například soubor, tvářící se jako hudební soubor ve formátu MP3, může obsahovat viry, červy, trojské koně a další. Pokud by byl stejný soubor zaslán e-mailem a příjemce by měl nainstalovaný antivirový program, soubor by byl před stažením do počítače prověřen, jeho pravá identita by byla odhalena a bylo by přijato nějaké bezpečnostní opatření. Například odstranění tohoto souboru. Sdílení souborů pomocí peer to peer aplikací ovšem takto nefunguje. Soubor se skrytým škodlivým softwarem je stahován z běžného FTP[10] serveru nebo HTTP a tím se vyhne kontrole antivirového programu. Tento soubor pak má volnou cesto k infikovaní systému. Tímto způsobem může také dojít k zavlečení škodlivého softwaru jako je například spyware [8].

Spyware využívá internet k odesílání dat bez vědomí jeho uživatele. Program typu spyware, odesílá především statistická data, například to jaké webové stránky uživatel navštěvuje, v jakém množství nebo jaké instaluje

[9] HTTP – HyperText Transfer Protocol
[10] FTP – File Transfer Protocol

programy. Takto získané informace jsou poté využívány pro cílenou reklamu. Příklad spyware:

- W32.D1der.Trojan - *Spyware schopný sledovat webové stránky, které uživatelé navštívili a přenést tuto informaci třetím stranám. Tento trojský kůň byl nalezen v v populárních P2P systémech jako jsou BearShare, LimeWare, Kazza [8].*
- Vx2.dll – Jeden z velmi nebezpečných spywarů, nalezený v několika verzích Audio Galaxy. Zaznamenává navštívené webové stránky, ale také dokáže zaznamenat údaje vložené do webových formulářů.

  Tato schopnost je zvláště potenciálně velmi nebezpečná, neboť touto cestou mohou uniknout velmi citlivé informace – čísla kreditních karet, hesla či čísla účtů [8].

  Další vlastností tohoto spywaru je vytváření vyskakovacích reklamních oken.

Třetím vážným problémem peer to peer sítí jsou tzv. DoS[11] útoky. DoS lze přeložit jako odmítnutí služby a jejich cílem je znepřístupnění určité služby, počítače, serveru nebo sítě. V současné době jsou nejpopulárnějšími DoS útoky, které se snaží využít nedostatečného zabezpečení jednotlivých aplikací. DoS útok začíná zpravidla tím, že si útočník prověří svoji oběť. Zjistí si jaký používá operační systém, dále jaké poskytuje síťové služby a jaké používá aplikace. Dalším jeho krokem je vyhledávání bezpečnostních chyb na internetu v aplikacích, které oběť používá. Tyto chyby může útočník snadno nalézt na http://www.osvdb.org . Na této adrese může útočník nalézt i tzv. exploit, které lze použít k provedení samotného DoS útoku.

Exploit je jednoúčelový program, který slouží k provedení útoku. Může být použit pro otestování zranitelnosti systému nebo pro studijní účely. Nejčastěji

[11] Denial of Service

je ovšem používán lidmi, kteří problematice vůbec nerozumí a pouze ho použijí k tomu. aby provedli někomu škodu. [9]

DoS útoky lze rozdělit na dvě hlavní části a to na, lokální DoS útoky – útočník musí mít přístup k napadenému počítači a vzdálené DoS útoky – počítač lze napadnout vzdáleně, protože bezpečnostní chyba toto útočníkovi umožňuje. Dále se můžeme také setkat s DDoS útoky, což jsou distribuované DoS útoky. DDoS útoky jsou založené na stejném principu jako DoS útoky, s jediným rozdílem a to, že útoků se účastní více počítačů najednou. Jako další příklady DoS útoků lze uvést DoS flood(záplavové) útoky, DoS útoky využívající MITM[12] útoky a mnoho dalších [9].

[12] Man in the middle

3.2 Bezpečnostní rizika peer to peer aplikací

Většina peer to peer aplikací v současné době požaduje po uživateli, aby sdílel vlastní data a to především jako preventivní opatření proti tzv. „pijavicím“, tedy uživatelům, kteří jen vysávají data z jiných uživatelů a sami nic nesdílejí. Tento fakt sebou nese určité riziko pro nepozorné uživatele. Starší verze peer to peer aplikací jako například Kazza měli defalutně sdílení disku vypnuté a bylo jen na uživateli jaká data bude sdílet. Zatímco současné verze peer to peer aplikací mají defalutně nastavené sdílení celého disku. Po té už je jen na uživateli, aby si tohoto faktu všiml a toto nastavení změnil. Zde vážně hrozí, že budou sdílená soukromá a systémová data a budou tak přístupna prakticky komukoliv [8].

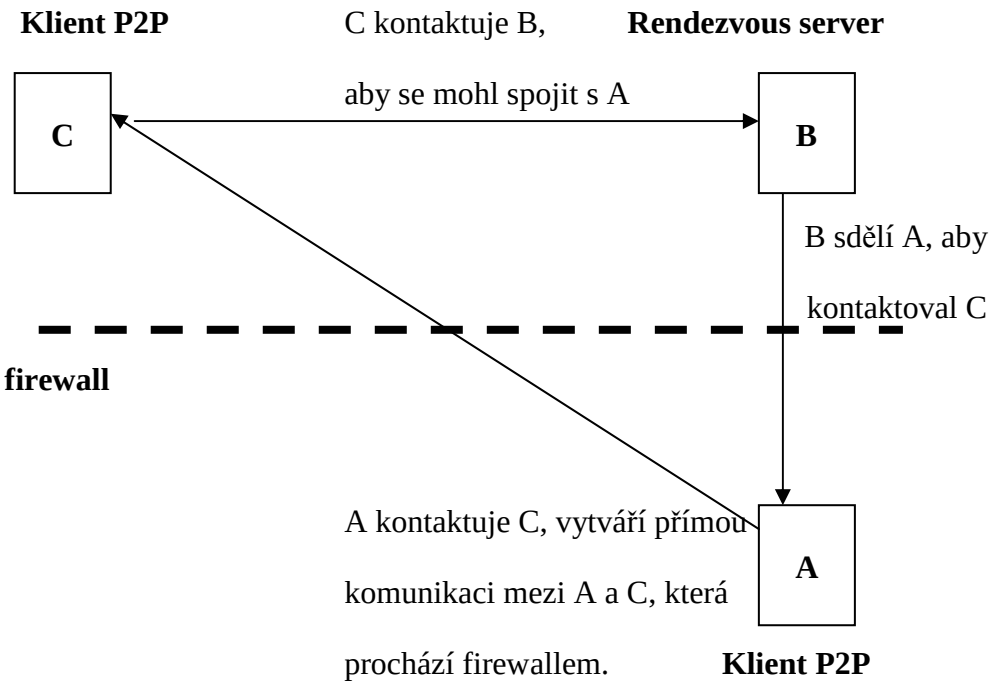
Další příklad rizikové funkce peer to peer aplikací je způsob inzerce v peer to peer systému Kazza.

Kazaa provádí inzerci v lokální zóně MSIE. To představuje bezpečnostní riziko, protože je zde možné do inzerátu propašovat škodlivý software, který umožní provádět některé příkazy na počítači účastníka nebo odhalit obsah systémových souborů. [8]

Jedno z největších rizik však představuje samotné chování uživatelů peer to peer aplikací. Ve většině firem je bez souhlasu pověřené osoby zakázané instalování jakéhokoliv softwaru a to hlavně peer to peer aplikací. Bohužel tento zákaz je velmi často ignorován a porušován. Velmi často uživatelé nedodržují bezpečností pravidla a neuvědomují si možná bezpečností rizika, která používání těchto aplikací přináší. V některých případech i samotní provozovatelé peer too peer aplikací poskytují uživatelům cenné rady jak obejít bezpečností opatření firem. Způsobů jak obejít ochranné síťové prvky je spousta. Jak již bylo zmíněno výše, velká část peer to peer aplikací využívá jako standardní protokol HTTP. Spojení přes protokol HTTP je většinou firewallů bez problémů přijato, je-li ovšem firewall správně nastaven spojení

inicované zvenčí přijato nebude. Ovšem i toto umějí peer to peer aplikace obejít a to způsobem, který popsal Ing. Ladislav Beránek.

Jeden přístup je založen na veřejně adresovatelném uzlu nazývaném rendezvous server, s kterým se účastnící chránění firewallem již mohou spojit. Takový uzel funguje jako prostředník, který umožní uzlu uvnitř sítě chráněné firewallem komunikaci s uzlem vně této sítě[8].



Obr. 3: Vytváření spojení mezi servery pomocí rendezvous serveru[8].

3.3 Bezpečnostní politika

Vzhledem k faktům, které jsou uvedeny a popsány výše, je zavedení bezpečnostní politiky týkající se používání peer to peer aplikací ve firmách a společnostech jednou z nejdůležitějších věcí pro osoby zodpovědné za bezpečnost. Téma bezpečnostních politik je relativně novou a ne příliš prozkoumanou oblastí. Osoby prověřené vytvořením bezpečnostní politiky se poté velmi často obrací k různým zdrojům již vypracovaných politik, například na internetu. Tato skutečnost vede k tomu, že takto navržená nebo zkopírovaná

bezpečnostní politika neodráží skutečné potřeby podniku v oblasti bezpečnosti sítí a otevírá tak prostor možným útočníkům a různým druhům útoků.

Jak již bylo zmíněno peer to peer aplikace, tedy dokáží velice snadno a rychle obejít klasické obranné prvky jako jsou například firewally. Nejefektivnější obranou je vše zabezpečit systémově, znemožnit uživatelům instalování jakýchkoli softwarových produktů a tuto oblast nechat pouze na kvalifikovaných pracovnících podnikového IT. Dále je žádoucí používat kvalitní a hlavně aktuální antivirový program. Velká váha se také klade na neustálé školení uživatelů.

Zdaleka největší množství bezpečnostních incidentů jde totiž na vrub nízkého bezpečnostního uvědomění a zanedbávání bezpečnostních procedur a opatření běžnými uživateli. Pokud uživatelé lépe rozumějí základnímu provoznímu a potenciálnímu riziku peer-to-peer systémů, budou lépe spolupracovat při dodržování bezpečnostních opatření[8].

4 Popis experimentu

4.1 Použitý hardware

Pro testování jednotlivých aplikací bylo nutné vytvořit si vlastní domácí síť. V síti byly použity tyto počítače:

Stanice č.1: Notebook MSI GX630X – 008CZ, procesor AMD Turion-X2 ZM-80, grafická karta nVidia GeForce 9600M GT, RAM DDR2 4096 MB.

Stanice č.2: Stolní PC, procesor AMD Sempron 2200+, grafická karta nVidia GeForce FX 5200, RAM 512 MB.

Stanice č.3: Netbook ASUS Eee PC 1201NL, procesor Intel Atom N270, grafická karta nVidia ION, RAM DDR2 2048 MB.

Stanice byly propojeny klasickým síťovým kabelem RJ45.

4.2 Použitý software

Nessus 4.2.1 – Nessus lze označit jako bezpečnostní scanner. Byl vyvinutý firmou Tenable Network Security. Nessus může být použit na jakémkoliv systému, uživatelské rozhraní je tvořené jednoduchým HTTP serverem a webovým klientem [10]. Tento software byl použit pro odhalení bezpečnostních chyb testovaných aplikací.

Dále následují testované aplikace, níže uvedené aplikace byly testovány samostatně a postupně na různých operačních systémech:

BitTorrent 7.1 – jednoduchý klient, který poskytuje pouze základní funkce pro stahování souborů s příponou ".torrent" z peer to peer sítí . BitTorrent je oficiální a originální klient od samotného tvůrce BitTorrent myšlenky. Je vytvořen pro operační systémy Windows XP, 2000, Vista a vyšší verze. Domovská stránka: http://www.bittorrent.com

BitComet 1.06 – klient pro stahování a sdílení souborů v peer to peer sítích, využívající technologii BitTorrentu, fungující na operačních systémech WinXP, Win2000, WinVista a vyšších. Nejnovější verze 1.23 obsahuje funkce chat s ostatními uživateli, integrovaný firewall, možnost blokování IP adres, kontrolu stahovaných souborů pomocí antivirového programu uživatele, automatické aktualizace a další. Oficiální stránky BitCometu: http://www.bitcomet.com/

Ares Galaxy 2.1.6 – klient pro stahování souborů využívající vlastní decentralizovanou peer to peer síť. Umožňuje také stahování a sdílení souborů v síti BitTorrent. Běží na všech systémech Windows od verze 98. Webové stránky programu: http://aresgalaxy.sourceforge.net/

StrongDC++ 2.41 – klient pro sdílené souborů v sítí Direct connect, hlavní funkce jsou segmentované stahování, částečné sdílení souborů, automatické odpojování pomalých stahování. Podporované systémy jsou všechny verze Windows. Domovská stránka aplikace: http://strongdc.sourceforge.net/

BearShare 6.2.0 – klient využívající síť Gnutella, podporuje stahování více kanály, vypalovaní audio CD, několikanásobné vyhledávání. Domovská stránka: http://www.bearshare.com/

Vuze 4.5.1 – klient napsaný v jazyce Java využívající síť BitTorrent, v této práci byla tato aplikace testována na linuxovém systému.

Deluge – také klient, který využívá síť BitTorrent. Je napsán v jazyce python. Tato aplikace byla také testována linuxovém systému.

Operační systémy: Windows2000, WindowsXP, WindowsXP_SP1, WindowsXP_SP2, WindowsXP_SP3, Windows Vista Business x86, Windows Vista Business_SP1, Windows Vista Business_SP2, Windows7, Linux – distribuce Ubuntu.

4.3 Popis experimentu

Po vytvoření sítě z výše uvedených počítačů byl na stanici č.1 spuštěn nessus, ze kterého probíhalo testování a na stanici č.2 byly postupně spouštěny testované aplikace a obměňovány operační systémy. Na stanici č.2 proběhlo testování na všech systémech s výjimkou Windows7, který byl testován na stanici č.3. Výše uvedené aplikace byly testovány nejprve na systému Windows 2000 s výjimkou BearSharu, který není určen pro tento systém a aplikace Vuze a Deluge, které byly testovány na linuxových systémech. Systém Windows 2000 nebyl nijak aktualizován a aplikace byly testovány ihned po jeho nainstalování na počítač. Dále proběhlo testování na systému Windows XP a to všech aplikací s výjimkou aplikace Vuze a Deluge. Systém WindowsXP byl postupně ošetřen service packy 1,2 a 3. Dalším systémem byl Windows Vista Business, testování aplikací zde proběhlo stejně jako na WindowsXP. Windows Vista Business byl také průběžně postupně ošetřen service packy 1 a 2. Posledním testovaným systémem od společnosti Microsoft byl Windows 7. Windows 7 byl testován plně aktualizovaný k 24. říjnu 2010. Pro porovnání se systémy Microsoft byl testování podroben také Linux, konkrétně distribuce Ubuntu 10.10. Na této distribuci byly otestovány aplikace BitTorrent, Vuze a Deluge. Výsledkem bylo velké množství bezpečnostích zpráv z bezpečnostního skeneru nessus. Vyhodnoceno a popsáno jich bylo celkem 47.

5 Výsledky experimentu

Z důvodů vysokého množství chyb budou popsány jen chyby s vysokým a středním rizikovým faktorem.

5.1 BitTorrent

Aplikace BitTorrent testovaná na systému Windows 2000. V tabulce číslo 1 vidíme počet otevřených portů, počty bezpečnostních chyb podle rizikového faktoru a celkové množství chyb.

Ot. porty	High	Medium	Low	Celkem
8	17	2	27	54

Tab. 1: Přehled chyb BitTorrentu ve Windows 2000

Port ▲	Protocol	SVC Name	Total	High	Medium	Low	Open Port
0	udp	general	1	0	0	1	0
0	tcp	general	11	2	0	9	0
0	icmp	general	1	0	0	1	0
135	tcp	epmap	4	1	0	1	2
135	udp	epmap?	1	1	0	0	0
137	udp	netbios-ns	1	0	0	1	0
139	tcp	smb	3	0	0	1	2
445	tcp	cifs	26	12	2	10	2
1025	tcp	dce-rpc	4	1	0	1	2
1026	udp	dce-rpc	1	0	0	1	0
1900	udp	upnp-client	1	0	0	1	0

Obr. 4: BitTorrent ve Windows 2000.

Na obrázku č.4 vidíme zprávu z nessusu, na kterém jsou vidět konkrétní porty, použité protokoly a počty chyb opět rozdělené podle rizikového faktoru. Vidíme že nejvíce chyb, celkem 12 se vyskytlo na portu 445 a to s kritickým

rizikovým faktorem. S tímto rizikovým faktorem se tyto chyby vyskytují i na portu 0, kde jsou tyto chyby 2, dále pak na portu 135 a 1025.

Plugin ID ▲	Name	Port	Severity
11110	MS02-045: Microsoft Windows SMB Protocol SMB_COM_TR/	cifs (445/tcp)	High
11808	MS03-026: Microsoft RPC Interface Buffer Overrun (823980)	cifs (445/tcp)	High
11835	MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (	cifs (445/tcp)	High
12054	MS04-007: ASN.1 Vulnerability Could Allow Code Execution (	cifs (445/tcp)	High
12209	MS04-011: Security Update for Microsoft Windows (835732) (	cifs (445/tcp)	High
18502	MS05-027: Vulnerability in SMB Could Allow Remote Code Ex	cifs (445/tcp)	High
19407	MS05-043: Vulnerability in Printer Spooler Service Could Allow	cifs (445/tcp)	High
19408	MS05-039: Vulnerability in Plug and Play Service Could Allow	cifs (445/tcp)	High
21193	MS05-047: Plug and Play Remote Code Execution and Local	cifs (445/tcp)	High
22034	MS06-035: Vulnerability in Server Service Could Allow Remote	cifs (445/tcp)	High
22194	MS06-040: Vulnerability in Server Service Could Allow Remote	cifs (445/tcp)	High
35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Cc	cifs (445/tcp)	High

Obr. 5: Chyby v BitTorrentu.

Na obrázku č.5 je zobrazen podrobný výpis chyb s kritickým nebo s vysokým rizikovým faktorem na portu 445, který byl získán opět z bezpečnostního skeneru nessus. Chyby jsou označeny pomocí Plugin ID a budou popsány na konci této kapitoly a to z důvodů výskytu stejných chyb u více aplikací. Dále budou chyby jen vypsány pomocí Plugin ID. Pro vyšší přehlednost budou chyby seřazeny od nejnižšího PluginID.

Nalezené chyby:

Port 0/TCP (High – 2x): PluginID 34477, 47709.

Port 135/TCP (High – 1x): PluginID 21655.

Port 135/UDP (High – 1x): PluginID 11890.

Port 445/TCP (High – 12x, Medium – 2x): PluginID 11110, 11808, 11835, 12054, 12209, 18502, 18585, 18602, 19407, 19408, 21193, 22034, 22194, 35362.

Port 1025/TCP (High – 1x): PluginID 13852.

Aplikace BitTorrent testovaná na systému Windows XP bez service packů.

Ot. porty	High	Medium	Low	Celkem
10	4	0	27	41

Tab. 2: Přehled chyb BitTorrentu ve Windows XP.

Nalezené chyby:

Port 0/TCP (High – 1x): PluginID 47709.

Port 135/UDP (High – 1x): PluginID 11890.

Port 445/TCP (High – 1x): PluginID 12209.

Port 1025/TCP (High – 1x): PluginID 13852.

V tabulce č. 2 vidíme, že o proti systému Windows 2000 došlo k výraznému snížení chyb s kritickým nebo vysokým rizikovým faktorem, je zde ovšem otevřeno více portů. Konkrétně se jedná o port 5000.

Aplikace BitTorrent testovaná na systému Windows XP ošetřeném service packem 1.

Ot. porty	High	Medium	Low	Celkem
10	4	0	27	41

Tab. 3: Přehled chyb BitTorrentu ve Windows XP-SP1.

Nalezené chyby:

Port 0/TCP (High – 1x): PluginID 47709.

Port 135/UDP (High – 1x): PluginID 11890.

Port 445/TCP (High – 1x): PluginID 12209.

Port 1025/TCP (High – 1x): PluginID 13852.

Po nainstalování service packu 1 je výsledek testováné aplikace BitTorrent téměř stejný jako u testování na systému bez service packu.

Aplikace BitTorrent testovaná na systému Windows XP ošetřeném service packem 2.

Ot. porty	High	Medium	Low	Celkem
6	5	0	17	28

Tab. 4: Přehled chyb BitTorrentu ve Windows XP-SP2.

Nalezené chyby:

Port 0/TCP (High – 1x): PluginID 34477.

Port 445/TCP (High – 4x): PluginID 18502, 22034, 22194, 35362.

Výsledkem nainstalování service packu 2 je snížení otevřených portů a chyb s nízkým rizikovým faktorem. Ovšem přibyla zde jedna chyba s kritickým rizikovým faktorem.

Aplikace BitTorrent testovaná na systému Windows XP ošetřeném service packem 3.

Ot. porty	High	Medium	Low	Celkem
6	2	0	16	24

Tab. 5: Přehled chyb BitTorrentu ve Windows XP-SP3.

Nalezené chyby:

Port 0/TCP (High – 1x): PluginID 34477.

Port 445/TCP (High – 1x): PluginID 35362.

Výsledkem nainstalování service packu 3 je opět snížení chyb se všemi rizikovými faktory.

Aplikace BitTorrent testovaná na systému Windows Vista bez ošetření service packy.

Ot. porty	High	Medium	Low	Celkem
6	1	0	24	31

Tab. 6: Přehled chyb BitTorrentu ve Windows Vista.

Nalezené chyby:

Port 445/TCP (High – 1x): PluginID 29855.

Aplikace BitTorrent testovaná na systému Windows Vista ošetřeném service packem 1.

Ot. porty	High	Medium	Low	Celkem
6	1	0	24	31

Tab. 7: Přehled chyb BitTorrentu ve Windows Vista-SP1.

Nalezené chyby:

Port 445/TCP (High – 1x): PluginID 40887.

Výsledek vypadá na první pohled stejný jako výsledek na systému bez ošetření service packem, jedná se ovšem o jinou chybu.

Aplikace BitTorrent testovaná na systému Windows Vista ošetřeném service packem 2.

Ot. porty	High	Medium	Low	Celkem
6	1	0	24	31

Tab. 8: Přehled chyb BitTorrentu ve Windows Vista-SP2.

Nalezené chyby:

Port 445/TCP (High – 1x): PluginID 40887.

Zde je výsledek stejný jako u testování v předchozím případě. V oblasti používání aplikace BitTorrent na systému Windows Vista nemá verze service packu žádný význam.

Aplikace BitTorrent testovaná na systému Windows 7.

Ot. porty	High	Medium	Low	Celkem
8	0	0	27	35

Tab. 9: Přehled chyb BitTorrentu ve Windows 7.

Zde vidíme, že na nejnovějším systému od firmy Microsoft, který je pravidelně aktualizovaný se nevyskytují žádné bezpečnostní chyby s kritickým, vysokým, nebo středním rizikovým faktorem.

5.2 BitComet

Aplikace BitComet testovaná na systému Windows 2000.

Ot. porty	High	Medium	Low	Celkem
8	17	2	26	53

Tab. 10: Přehled chyb BitCometu ve Windows 2000.

Nalezené chyby:

Port 0/TCP (High – 2x): PluginID 34477, 47709.

Port 135/TCP (High – 1x): PluginID 21655.

Port 135/UDP (High – 1x): PluginID 11890.

Port 445/TCP (High – 12x, Medium – 2x): PluginID 11110, 11808, 11835, 12054, 12209, 18502, 18585, 18602, 19407, 19408, 21193, 22034, 22194, 35362.

Port 1025/TCP (High – 1x): PluginID 13852.

V tabulce číslo 10 vidíme, že chyby které se vyskytují na aplikaci BitComet jsou téměř stejné jako na aplikaci BitTorrent. Rozdíly jsou jen v chybách s nízkým rizikovým faktorem, kterým se zde věnovat nebudeme. Chyby jsou si velmi podobné i v dalších testech. Proto dál bude následovat jen stručný výpis chyb s občasnými komentáři.

Aplikace BitComet testovaná na systému Windows XP.

Ot. porty	High	Medium	Low	Celkem
10	13	1	26	50

Tab. 11: Přehled chyb BitCometu ve Windows XP.

Nalezené chyby:

Port 0/TCP (High – 1x): PluginID 34477.

Port 135/UDP (High – 1x): PluginID 11890.

Port 135/TCP (High – 1x): PluginID 21655.

Port 445/TCP (High – 9x, Medium – 1x): PluginID 11808, 11835, 12054, 12209, 16337, 18502, 19407, 22034, 22194, 35362.

Port 1025/TCP (High – 1x): PluginID 13852.

V tabulce č. 11 ovšem vidíme více chyb s vysokým rizikovým faktorem, než tomu bylo u aplikace BitTorrent. BitTorrent byla jediná aplikace, který se v testování na systému Windows XP výrazněji lišila od ostatních.

Aplikace BitComet testovaná na systému Windows XP ošetřeném service packem 1.

Ot. porty	High	Medium	Low	Celkem
10	13	1	26	50

Tab. 12: Přehled chyb BitCometu ve Windows XP-SP1.

Nalezené chyby:

Port 0/TCP (High – 1x): PluginID 34477.

Port 135/UDP (High – 1x): PluginID 11890.

Port 135/TCP (High – 1x): PluginID 21655.

Port 445/TCP (High – 9x, Medium – 1x): PluginID 11808, 11835, 12054, 12209, 16337, 18502, 19407, 22034, 22194, 35362.

Port 1025/TCP (High – 1x): PluginID 13852.

V tabulce č. 12 platí opět to samé. Aplikace BitComet si zde vedla mnohem hůře než aplikace BitTorrent. Ovšem rozdíl mezi tím, zda byl použit service pack 1 je minimální.

Aplikace BitComet testovaná na systému Windows XP ošetřeném service packem 2.

Ot. porty	High	Medium	Low	Celkem
6	5	0	16	27

Tab. 13: Přehled chyb BitCometu ve Windows XP-SP2.

Nalezené chyby:

Port 0/TCP (High – 1x): PluginID 34477.

Port 445/TCP (High – 4x): PluginID 18502, 22034, 22194, 35362.

Zde již není mezi aplikacemi BitComet a BitTorrent výraznější rozdíl. Aplikace jsou si zase velmi podobné.

Aplikace BitComet testovaná na systému Windows XP ošetřeném service packem 3.

Ot. porty	High	Medium	Low	Celkem
6	2	0	16	24

Tab. 14: Přehled chyb BitCometu ve Windows XP-SP3.

Nalezené chyby:

Port 0/TCP (High – 1x): PluginID 34477.

Port 445/TCP (High – 4x): PluginID 35362.

Aplikace BitComet testovaná na systému Windows Vista.

Ot. porty	High	Medium	Low	Celkem
6	1	0	25	32

Tab. 15: Přehled chyb BitCometu ve Windows Vista.

Nalezené chyby:

Port 445/TCP (High – 4x): PluginID 29855.

Aplikace BitComet testovaná na systému Windows Vista ošetřeném service packem 1.

Ot. porty	High	Medium	Low	Celkem
6	1	0	24	31

Tab. 16: Přehled chyb BitCometu ve Windows Vista-SP1.

Nalezené chyby:

Port 445/TCP (High – 4x): PluginID 40887.

Aplikace BitComet testovaná na systému Windows Vista ošetřeném service packem 2.

Ot. porty	High	Medium	Low	Celkem
6	1	0	24	31

Tab. 17: Přehled chyb BitCometu ve Windows Vista-SP2.

Nalezené chyby:

Port 445/TCP (High – 4x): PluginID 40887.

Aplikace BitComet testovaná na systému Windows 7.

Ot. porty	High	Medium	Low	Celkem
8	0	0	27	35

Tab. 18: Přehled chyb BitCometu ve Windows 7.

5.3 Ares

Aplikace Ares testovaná na systému Windows 2000.

Ot. porty	High	Medium	Low	Celkem
8	17	2	26	53

Tab. 19: Přehled chyb Ares ve Windows 2000.

Nalezené chyby:

Port 0/TCP (High – 2x): PluginID 34477, 47709.

Port 135/TCP (High – 1x): PluginID 21655.

Port 135/UDP (High – 1x): PluginID 11890.

Port 445/TCP (High – 12x, Medium – 2x): PluginID 11110, 11808, 11835, 12054, 12209, 18502, 18585, 18602, 19407, 19408, 21193, 22034, 22194, 35362.

Port 1025/TCP (High – 1x): PluginID 13852.

Aplikace Ares testovaná na systému Windows XP.

Ot. porty	High	Medium	Low	Celkem
10	13	1	26	50

Tab. 20: Přehled chyb Ares ve Windows XP.

Nalezené chyby:

Port 0/TCP (High – 1x): PluginID 34477.

Port 135/UDP (High – 1x): PluginID 11890.

Port 135/TCP (High – 1x): PluginID 21655.

Port 445/TCP (High – 9x, Medium – 1x): PluginID 11808, 11835, 12054, 12209, 16337, 18502, 19407, 22034, 22194, 35362.

Port 1025/TCP (High – 1x): PluginID 13852.

Aplikace Ares testovaná na systému Windows XP ošetřeném service packem 1.

Ot. porty	High	Medium	Low	Celkem
10	13	1	26	50

Tab. 21: Přehled chyb Ares ve Windows XP-SP1.

Nalezené chyby:

Port 0/TCP (High – 1x): PluginID 34477.

Port 135/UDP (High – 1x): PluginID 11890.

Port 135/TCP (High – 1x): PluginID 21655.

Port 445/TCP (High – 9x, Medium – 1x): PluginID 11808, 11835, 12054, 12209, 16337, 18502, 19407, 22034, 22194, 35362.

Port 1025/TCP (High – 1x): PluginID 13852.

Aplikace Ares testovaná na systému Windows XP ošetřeném service packem 2.

Ot. porty	High	Medium	Low	Celkem
6	5	0	16	27

Tab. 22: Přehled chyb Ares ve Windows XP-SP2.

Nalezené chyby:

Port 0/TCP (High – 1x): PluginID 34477.

Port 445/TCP (High – 4x): PluginID 18502, 22034, 22194, 35362.

Aplikace Ares testovaná na systému Windows XP ošetřeném service packem 3.

Ot. porty	High	Medium	Low	Celkem
6	2	0	16	24

Tab. 23: Přehled chyb Ares ve Windows XP-SP3.

Nalezené chyby:

Port 0/TCP (High – 1x): PluginID 34477.

Port 445/TCP (High – 4x): PluginID 35362.

Aplikace Ares testovaná na systému Windows Vista.

Ot. porty	High	Medium	Low	Celkem
6	1	0	24	31

Tab. 24: Přehled chyb Ares ve Windows Vista.

Nalezené chyby:

Port 445/TCP (High – 4x): PluginID 29855.

Aplikace Ares testovaná na systému Windows Vista ošetřeném service packem 1.

Ot. porty	High	Medium	Low	Celkem
6	1	0	24	31

Tab. 25: Přehled chyb Ares ve Windows Vista-SP1.

Nalezené chyby:

Port 445/TCP (High – 4x): PluginID 40887.

Aplikace Ares testovaná na systému Windows Vista ošetřeném service packem 2.

Ot. porty	High	Medium	Low	Celkem
6	1	0	24	31

Tab. 26: Přehled chyb Ares ve Windows Vista-SP2.

Nalezené chyby:

Port 445/TCP (High – 4x): PluginID 40887.

Aplikace Ares testovaná na systému Windows 7.

Ot. porty	High	Medium	Low	Celkem
10	0	0	23	33

Tab. 27: Přehled chyb Ares ve Windows 7.

Aplikace Ares je opět velmi podobná aplikaci BitComet a také aplikaci BitTorrent s výjimkou systému Windows XP, kde si BitTorrent vedl o něco lépe.

5.4 StrongDC++

Aplikace StrongDC testovaná na systému Windows 2000.

Ot. porty	High	Medium	Low	Celkem
12	17	2	26	57

Tab. 28: Přehled chyb StrongDC ve Windows 2000.

Nalezené chyby:

Port 0/TCP (High – 2x): PluginID 34477, 47709.

Port 135/UDP (High – 1x): PluginID 11890.

Port 135/TCP (High – 1x): PluginID 21655.

Port 445/TCP (High – 12x, Medium – 2x): PluginID 11110, 11808, 11835, 12054, 12209, 18502, 18585, 18602, 19407, 19408, 21193, 22034, 22194, 35362

Port 1025/TCP (High – 1x): PluginID 13852.

Aplikace StrongDC testovaná na systému Windows XP.

Ot. porty	High	Medium	Low	Celkem
10	14	1	26	51

Tab. 29: Přehled chyb StrongDC ve Windows XP.

Nalezené chyby:

Port 0/TCP (High – 2x): PluginID 34477, 47709.

Port 135/UDP (High – 1x): PluginID 11890.

Port 135/TCP (High – 1x): PluginID 21655.

Port 445/TCP (High – 9x, Medium – 1x): PluginID 11808, 11835, 12054, 12209, 16337, 18502, 19407, 22034, 21194, 35362

Port 1025/TCP (High – 1x): PluginID 13852.

Aplikace StrongDC testovaná na systému Windows XP ošetřeném service packem 1.

Ot. porty	High	Medium	Low	Celkem
10	13	1	26	50

Tab. 30: Přehled chyb Ares ve Windows XP-SP1.

Nalezené chyby:

Port 0/TCP (High – 1x): PluginID 34477.

Port 135/UDP (High – 1x): PluginID 11890.

Port 135/TCP (High – 1x): PluginID 21655.

Port 445/TCP (High – 9x, Medium – 1x): PluginID 11808, 11835, 12054, 12209, 16337, 18502, 19407, 22034, 22194, 35362.

Port 1025/TCP (High – 1x): PluginID 13852.

Aplikace StrongDC testovaná na systému Windows XP ošetřeném service packem 2.

Ot. porty	High	Medium	Low	Celkem
6	5	0	16	27

Tab. 31: Přehled chyb Ares ve Windows XP-SP2.

Nalezené chyby:

Port 0/TCP (High – 1x): PluginID 34477.

Port 445/TCP (High – 4x): PluginID 18502, 22034, 22194, 35362.

Aplikace StrongDC testovaná na systému Windows XP ošetřeném service packem 3.

Ot. porty	High	Medium	Low	Celkem
8	2	0	16	26

Tab. 32: Přehled chyb Ares ve Windows XP-SP3.

Nalezené chyby:

Port 0/TCP (High – 1x): PluginID 34477.

Port 445/TCP (High – 1x): PluginID 35362.

Aplikace StrongDC testovaná na systému Windows Vista.

Ot. porty	High	Medium	Low	Celkem
6	1	0	24	31

Tab. 33: Přehled chyb StrongDC ve Windows Vista.

Nalezené chyby:

Port 445/TCP (High – 1x): PluginID 29855.

Aplikace StrongDC testovaná na systému Windows Vista ošetřeném service packem 1.

Ot. porty	High	Medium	Low	Celkem
6	1	0	24	31

Tab. 34: Přehled chyb StrongDC ve Windows Vista-SP1.

Nalezené chyby:

Port 445/TCP (High – 1x): PluginID 40887.

Aplikace StrongDC testovaná na systému Windows Vista ošetřeném service packem 2.

Ot. porty	High	Medium	Low	Celkem
6	1	0	24	31

Tab. 35: Přehled chyb StrongDC ve Windows Vista-SP2.

Nalezené chyby:

Port 445/TCP (High – 1x): PluginID 40887.

Aplikace StrongDC testovaná na systému Windows 7.

Ot. porty	High	Medium	Low	Celkem
8	0	0	27	35

Tab. 36: Přehled chyb StrongDC ve Windows 7.

Aplikace StrongDC, si vedla podobně jako aplikace Ares a BitComet.

5.5 BearShare

Aplikace BearShare nebyla na systému Windows 2000 testovaná. Použitá verze BearShare nebyla kompatibilní s daným operačním systémem a tudíž nešla spustit.

Aplikace BearShare testovaná na systému Windows XP.

Ot. porty	High	Medium	Low	Celkem
12	13	1	27	53

Tab. 37: Přehled chyb BearShare ve Windows XP.

Nalezené chyby:

Port 0/TCP (High – 1x): PluginID 34477.

Port 135/UDP (High – 1x): PluginID 11890.

Port 135/TCP (High – 1x): PluginID 21655.

Port 445/TCP (High – 9x, Medium – 1x): PluginID 11808, 11835, 12054, 12209, 16337, 18502, 19407, 22034, 21194, 35362

Port 1025/TCP (High – 1x): PluginID 13852.

Aplikace BearShare testovaná na systému Windows XP ošetřeném service packem 1.

Ot. porty	High	Medium	Low	Celkem
10	13	1	26	50

Tab. 38: Přehled chyb BearShare ve Windows XP-SP1.

Nalezené chyby:

Port 0/TCP (High – 1x): PluginID 34477.

Port 135/UDP (High – 1x): PluginID 11890.

Port 135/TCP (High – 1x): PluginID 21655.

Port 445/TCP (High – 9x, Medium – 1x): PluginID 11808, 11835, 12054, 12209, 16337, 18502, 19407, 22034, 22194, 35362.

Port 1025/TCP (High – 1x): PluginID 13852

Aplikace BearShare testovaná na systému Windows XP ošetřeném service packem 2.

Ot. porty	High	Medium	Low	Celkem
6	5	0	16	27

Tab. 39: Přehled chyb BearShare ve Windows XP-SP2.

Nalezené chyby:

Port 0/TCP (High – 1x): PluginID 34477.

Port 445/TCP (High – 4x): PluginID 18502, 22034, 22194, 35362.

Aplikace BearShare testovaná na systému Windows XP ošetřeném service packem 3.

Ot. porty	High	Medium	Low	Celkem
6	2	0	16	24

Tab. 40: Přehled chyb BearShare ve Windows XP-SP3.

Nalezené chyby:

Port 0/TCP (High – 1x): PluginID 34477.

Port 445/TCP (High – 1x): PluginID 35362.

Aplikace BearShare testovaná na systému Windows Vista.

Ot. porty	High	Medium	Low	Celkem
6	1	0	23	30

Tab. 41: Přehled chyb BearShare ve Windows Vista.

Nalezené chyby:

Port 445/TCP (High – 1x): PluginID 29855.

Aplikace BearShare testovaná na systému Windows Vista ošetřeném service packem 1.

Ot. porty	High	Medium	Low	Celkem
6	1	0	24	31

Tab. 42: Přehled chyb BearShare ve Windows Vista-SP1.

Nalezené chyby:

Port 445/TCP (High – 1x): PluginID 40887.

Aplikace BearShare testovaná na systému Windows Vista ošetřeném service packem 2.

Ot. porty	High	Medium	Low	Celkem
6	1	0	24	31

Tab. 43: Přehled chyb BearShare ve Windows Vista-SP2.

Nalezené chyby:

Port 445/TCP (High – 1x): PluginID 40887.

Aplikace BearShare testovaná na systému Windows 7.

Ot. porty	High	Medium	Low	Celkem
8	0	0	27	35

Tab. 44: Přehled chyb BearShare ve Windows 7.

Aplikace BearShare, si vedla podobně jako aplikace Ares, BitComet a StrongDC.

5.6 Testování aplikací na Linuxu

Na linuxu byly testovány tři následující aplikace. BitTorrent, Vuze a Deluge. U aplikace BitTorrent bude tedy možné porovnat její bezpečnost na odlišných typech operačních systémů.

Aplikace BitTorrent

Ot. porty	High	Medium	Low	Celkem
0	0	1	5	6

Tab. 45: Přehled chyb BitTorrent na Linuxu.

Aplikace Vuze

Ot. porty	High	Medium	Low	Celkem
0	0	1	5	6

Tab. 46: Přehled chyb Vuze na Linuxu.

Aplikace Deluge

Ot. porty	High	Medium	Low	Celkem
0	0	1	5	6

Tab. 47: Přehled chyb Vuze na Linuxu.

V tabulkách č. 45, 46 a 47 vidíme, že výsledky testovaných aplikací jsou stejné. Stejně jako na systémech od firmy Microsoft, mezi použitými aplikacemi není téměř žádný rozdíl. Pokud budeme porovnávat výsledky na úrovni použitého systému, na první pohled dopadl Linux lépe, než systémy Microsoft. Tento fakt, lze přisoudit tomu, že systému Linux nepoužívá takové množství uživatelů jako systémy od firmy Microsoft, tím pádem je na ně vedeno méně útoků. Pro lepší závěry by bylo vhodné tyto aplikace vyzkoušet i na dalších distribucích Linuxu.

5.7 Popis nalezených chyb

Plugin ID:

11110 – Rizikový faktor vysoký. Vzdálený hostitel je zranitelný DOS útoky na jeho SMB stack. Útočník může tuto chybu vzdáleně využít k havárii vzdáleného hostitele, bez jakékoli autorizace nebo oprávnění.

Řešení – Použít odpovídající záplaty (MS02-045) nebo instalovat nejnovější Windows service packy.

11808 – Rizikový faktor kritický. Vzdálená verze operačního systému Windows obsahuje chybu ve funkci RemoteActivation() v rozhraní RPC[13], která umožňuje útočníkovi spustit jakýkoli kód se systémovými právy. Série červů Blaster je známá právě využíváním této chyby.

Řešení – Doporučení jak řešit tuto chybu a další informace lze nalézt na níže uvedené adrese. http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx

11835 – Rizikový faktor kritický. Na vzdáleném hostiteli je spuštěna verze systému Windows, která obsahuje chybu v rozhraní RPC, která může opět útočníkovi povolit spuštění libovolného kódu a získat tak systémová oprávnění. Útočník nebo červ toto mohou využít k získání kontroly nad tímto hostitelem. Nejedná se o stejnou chybu, která je popsána výše a která opravuje chybu využívanou červi MSBlast nebo LoveSan.

Řešení – Doporučení jak řešit tuto chybu lze nalézt na níže uvedené adrese. http://www.microsoft.com/technet/security/bulletin/MS03-039.mspx

11890 – Rizikový faktor kritický. Ve službě Messenger existuje slabé místo v zabezpečení, které útočníkovi umožňuje spuštění jakéhokoli kódu v napadeném systému. Útočník, který by úspěšně tuto chybu využil by byl schopen libovolný kód spustit se všemi oprávněními místního systému nebo způsobit pád služby Messenger. Pravděpodobnost tohoto útoků se dá snížit preventivním vypnutím služby Messenger.

Řešení – společnost Microsoft vydala sadu bezpečnostních záplat pro Windows 2000, XP a 2003.

12054 – Rizikový faktor kritický. Vzdálený hostitel používající systém Windows má knihovnu ASN.1[14], která může útočníkovi umožnit spuštění

[13] RPC - Remote Procedure Call – vzdálené volání procedur
[14] ASN.1 – Abstraktní Syntaktická Notace verze 1

jakéhokoli kódu na tomto hostiteli. K využití této chyby by musel útočník odeslat speciální vytvořený a zakódovaný packet ASN.1 s nesprávně inzerovanou délkou.

Řešení – Doporučení jak řešit tuto chybu a další informace lze nalézt na níže uvedené adrese. http://www.microsoft.com/technet/security/bulletin/ms04-007.mspx

12209 – Rizikový faktor kritický. Vzdálená verze systému Windows obsahuje chybu ve funkci DsRolerUpgradeDownlevelServer z LSASS[15]. Tato chyba může opět útočníkovi spustit libovolný kód se systémovými oprávněními. Tuto chybu využívá hlavně série červů Sasser.

Řešení – společnost Microsoft vydala sadu bezpečnostních záplat pro Windows 2000, XP a 2003. Další informace lze získat na http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx

12218 – Rizikový faktor střední. Tato chyba, byla nalezena jako jediná na systému Linux. Vzdálená služba chápající protokol Bonjour známý také jako ZeroConf nebo mDNS, umožňuje odkrýt důležité informace o vzdáleném hostiteli. Například jeho typ operačního systému a jeho přesnou verzi, jeho hostname a seznam spuštěných aplikací.

Řešení – Filtrování provozu na portu 5353 UDP.

13852 – Rizikový faktor kritický. Zde je chyba v aplikaci Task Scheduler (plánovač úloh), která umožní útočníkovi vzdálené spuštění kódu. Existuje mnoho útoků, které využívají tuto chybu. Útočník využívající tuto chybu potřebuje mít přímé spojení k cílovému počítači nebo musí uživatele donutit buď nainstalovat soubor .job nebo navštívit škodlivé webové stránky.

[15] LSASS – Local Security Autority Server Service

Řešení – společnost Microsoft vydala sadu bezpečnostních záplat pro Windows 2000, XP a 2003. Další informace o tomto problému lze nalézt na adrese http://www.microsoft.com/technet/security/bulletin/ms04-022.mspx

16337 – Rizikový faktor střední. Vzdálená verze Windows obsahuje chybu, která může pomoci útočníkovi odhalit informace, které může využít pro získání podrobnějších informací o hostiteli k jeho další útokům.

Řešení – společnost Microsoft vydala sadu bezpečnostních záplat pro Windows XP. Další informace týkající se tohoto problému lze najít zde http://www.microsoft.com/technet/security/bulletin/ms05-007.mspx

18502 – Rizikový faktor kritický. Vzdálená verze systému Windows obsahuje chybu v implementaci protokolu SMB[16]. Tato chyba umožňuje útočníkovi spustit libovolný kód na vzdáleném hostiteli. K zneužití této chyby útočník nepotřebuje žádnou autentifikaci.

Řešení – společnost Microsoft vydala sadu bezpečnostních záplat pro Windows 2000, XP a 2003.

18585 – Rizikový faktor střední. Pomocí použitého pluginu, který se připojí k \srvsvc získá útočník seznam běžících aplikací na vzdáleném hostiteli. Získané informace může útočník využít k dalšímu a lepšímu napadení vzdáleného hostitele.

Řešení – Chybu lze odstranit nainstalováním URP1[17] pro Windows 2000 SP4. Další informace o tomto problému lze nalézt na níže uvedené adrese http://www.hsc.fr/ressources/presentations/null_sessions/

18602 – Rizikový faktor střední. Na vzdálením hostiteli Windows 2000, lze anonymně číst event logy (protokoly událostí) připojením přes \srvsvc propojeným a svázaným se službou event log, OpenEventLog(). Útočník může

[16] SMB – Server Message Block – komunikační protkol sloužící k sdílenému přístupu k souborům, sériovým portům a tiskárnám.
[17] URP1 – Update Rollup Package 1

tuto chybu využít k anonymnímu čtení systémových logů vzdáleného hostitele. Tyto logy obsahují důležité informace, které může útočník využít k dalším a lepším útokům proti vzdálenému hostiteli.

Řešení – Chybu lze odstranit nainstalováním URP1 pro Windows 2000 SP4 nebo nastavením hodnoty RestrictGuestAccess na Applications and System logs. Další informace týkající se této problematiky lze nalézt na http://archives.neohapsis.com/archives/fulldisclosure/2005-07/0137.html

19407 – Rizikový faktor kritický. Vzdálený hostitel používá verzi služby Print Spooler, která může útočníkovi umožnit spuštění jakéhokoli kódu nebo pád této služby.

Řešení – společnost Microsoft vydala sadu bezpečnostních záplat pro Windows 2000, XP a 2003.

19408 – Rizikový faktor kritický. Vzdálená verze systému Windows obsahuje chybu ve funkci PNP_QueryResConfList() používanou službou Plug and Play, která může útočníkovi umožnit spuštění jakéhokoli kódu na vzdáleném hostiteli se systémovými právy. Tento nedostatek v zabezpečení využívá série červů Zotob.

Řešení – společnost Microsoft vydala sadu bezpečnostních záplat pro Windows 2000, XP a 2003. Více informací lze nalézt na níže uvedené adrese http://www.microsoft.com/technet/security/bulletin/ms05-039.mspx

21193 – Rizikový faktor kritický. Vzdálený hostitel používá verzi služby Plug and Play, která obsahuje bezpečností nedostatky ve způsobu jakým ovládá uživatelem poskytnutá data. Autentifikovaný útočník může tuto chybu využít odesláním chybným RPC požadavkem na vzdálenou službu a tím spustit kód se systémovými právy. Výjimkou je Windows 2000, kde útočník nemusí být autentifikovaný, pokud systém není opraven patchem MS05-039.

Řešení – společnost Microsoft vydala sadu bezpečnostních záplat pro Windows 2000, XP.

21655 – Rizikový faktor kritický. Vzdálený hostitel má mnoho chyb v implementaci RPC/DCOM[18]. Útočník může využít jednu z těchto chyb ke spuštění libovolného kódu na vzdáleném systému.

Řešení – společnost Microsoft vydala sadu bezpečnostních záplat pro Windows 2000, XP a 2003.

22034 – Rizikový faktor vysoký. Vzdálený hostitel je zranitelný přetečením heapu (haldy) ve službě "Server". Tento bezpečností nedostatek může útočníkovi umožnit spuštění libovolného kódu na vzdáleném hostiteli se systémovými právy. Dále je hostitel ovlivněn také možností prozrazení informací z SMB, které mohou útočníkovi pomoct získat část paměti hostitele.

Řešení – společnost Microsoft vydala sadu bezpečnostních záplat pro Windows 2000, XP a 2003. Další informace lze nalézt na níže uvedené adrese http://www.microsoft.com/technet/security/bulletin/ms06-035.mspx

22194 – Rizikový faktor kritický. Vzdálený hostitel je zranitelný přetečením bufferu ve službě "Server", to může opět útočníkovi umožnit spuštění jakéhokoli kódu na vzdáleném hostiteli se systémovými právy.

Řešení – společnost Microsoft vydala sadu bezpečnostních záplat pro Windows 2000, XP a 2003.

29855 – Rizikový faktor kritický. Vzdálená verze Windows obsahuje protokol SMB2, který je ovlivněný několika bezpečnostními chybami. Útočník má možnost využít tyto chyby, zvýšit své práva a převzít kontrolu nad vzdáleným hostitelem.

Řešení – společnost Microsoft vydala sadu bezpečnostních záplat pro Windows Vista. Další informace týkající se tohoto problému lze nalézt na http://www.microsoft.com/technet/security/bulletin/ms07-063.mspx

---

[18] DCOM – Distributed Component Object Model – protokol, který definuje interakci mezi komponentami a jejich klienty.

34477 – Rizikový faktor kritický. Je prakticky stejná jako chyba č. 22194 akorát s rozdílem, že se vyskytuje na jiném portu a to na portu 0.

35362 – Rizikový faktor kritický. Vzdálený hostitel je ovlivněný možným poškozením paměti v SMB. Toto může vézt k spuštění jakéhokoli kódu nebo k DOS útokům proti vzdáleném hostiteli.

Řešení – společnost Microsoft vydala sadu bezpečnostních záplat pro Windows 2000, XP, 2003, Vista a 2008.

40887 – Rizikový faktor kritický. Na vzdáleném hostiteli je spuštěn systém Windows Vista, který obsahuje bezpečností chyby v implementaci SMB2. Útočník může tuto chybu využít k vyřazení vzdáleného hostitele nebo k spuštění libovolného kódu.

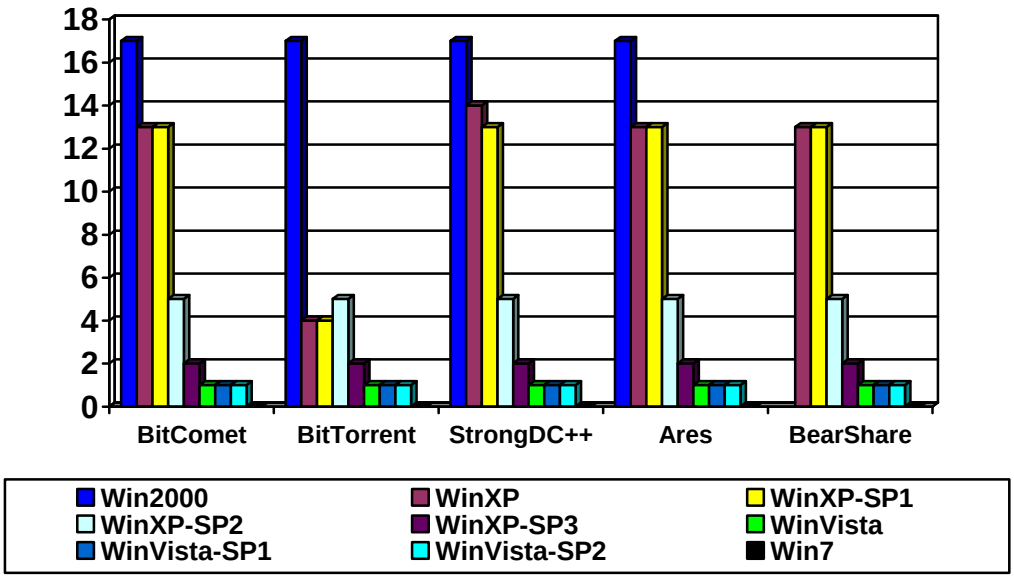
Řešení – společnost Microsoft vydala sadu bezpečnostních záplat pro Windows Vista a Windows Server 2008. Další informace lze nalézt na http://www.microsoft.com/technet/security/Bulletin/MS09-050.mspx

47709 – Rizikový faktor kritický. Na vzdáleném hostiteli běží systém Windows 2000. Tento operační systém již není podporován společností Microsoft, tedy pro něho neexistují žádné bezpečností aktualizace. Dalším problémem je nízká pravděpodobnost, že firma Microsoft odhalí nové chyby a útoky vedené proti tomuto systému.

Řešení – Nainstalovat vyšší verzi systému Windows.

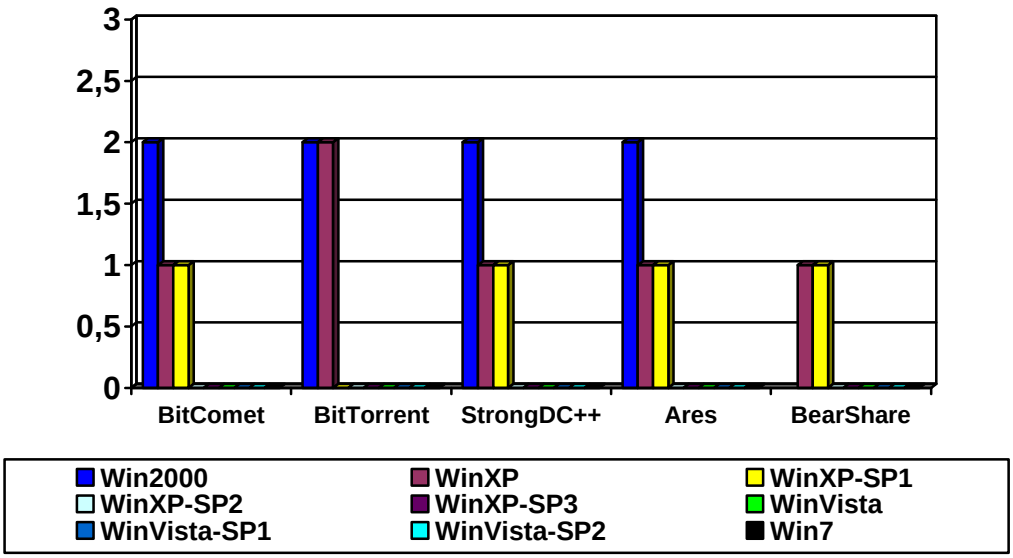
5.8 Shrnutí

Přehled bezpečnostních chyb s vysokým nebo kritickým rizikovým faktorem všech testovaných aplikací na všech operačních systémech je zobrazen na obr.7 (BearShare nebyl na systému Windows 2000 testován). Jak již bylo zmíněno výsledky všech aplikací jsou si velice podobné. Výjimkou je pouze aplikace BitTorrent na systému Windows XP, kde bylo odhaleno téměř o polovinu méně chyb než u ostatních aplikací.



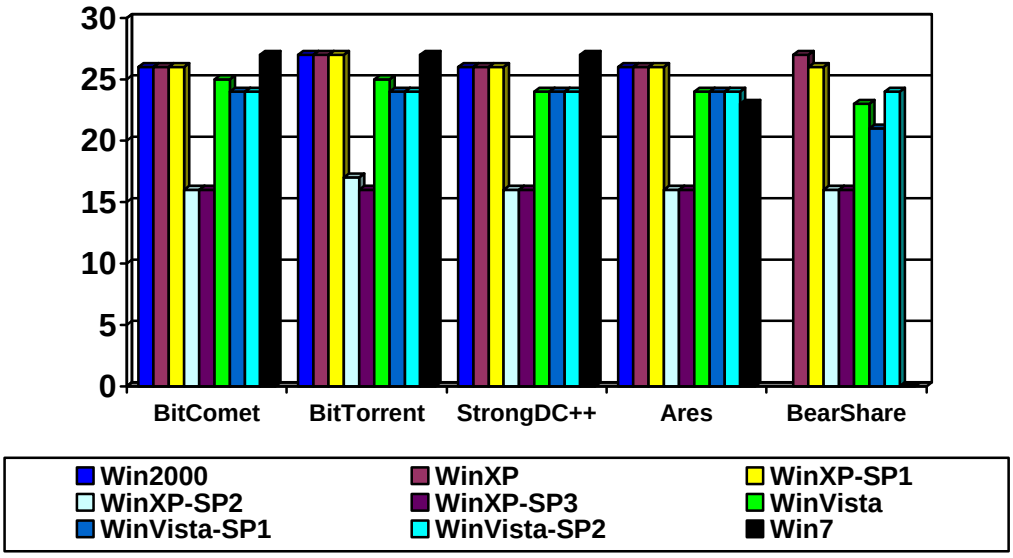
obr. 7: chyby s vysokým a kritickým rizikovým faktorem.

Na obr. 8 je zobrazen přehled chyb se středním rizikovým faktorem testovaných aplikací. Výsledky ukazují, že i zde jsou si aplikace velice podobné. Výjimku tvoří opět jen aplikace BitTorrent.



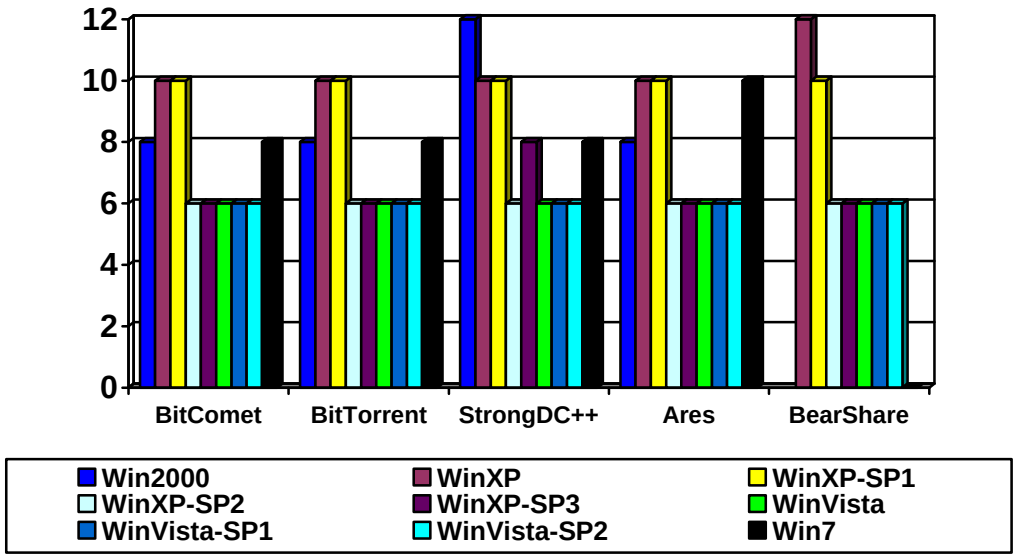
obr. 8: chyby se středním rizikovým faktorem.

Na obr. 9 je zobrazen přehled chyb s nízkým rizikovým faktorem. Zde jsou na první pohled vidět nějaký odlišnosti v testovaných aplikacích. Ovšem chybami s nízkým rizikovým faktorem, jsme se v této práci nezabývali. Výsledky jsou zde pouze informativní.



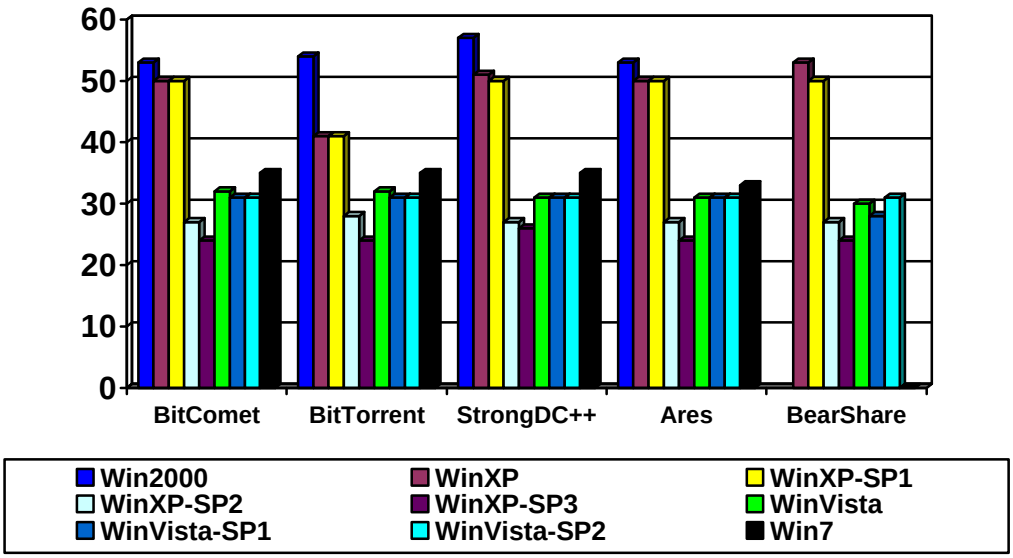
obr. 9: chyby s nízkým rizikovým faktorem.

Na obr. 10 je přehled otevřených portů. Tato informace je zde uvedena také pouze jako informativní.



obr. 10: počet otevřených portů.

Na obr. 11 je zobrazen celkový počet chyb testovaných aplikací. Z tohoto grafu lze usoudit, že nejméně chyb se nacházelo na systému Windows XP ošetřeném service packem 3, tedy systém který byl nejvíce aktualizován. Dále pak systém Windows Vista a Windows 7. Musíme však brát v potaz, že v celkovém počtu chyb jsou nejvíce zastoupeny chyby s nízkým rizikovým faktorem, hlavně u systémů které byly ošetřeny vyššími verzemi service packů.



obr. 11: celkový počet chyb.

6 Průzkum používání a rizik peer to peer aplikací v podnicích

6.1 Cíl průzkumu a předpoklady

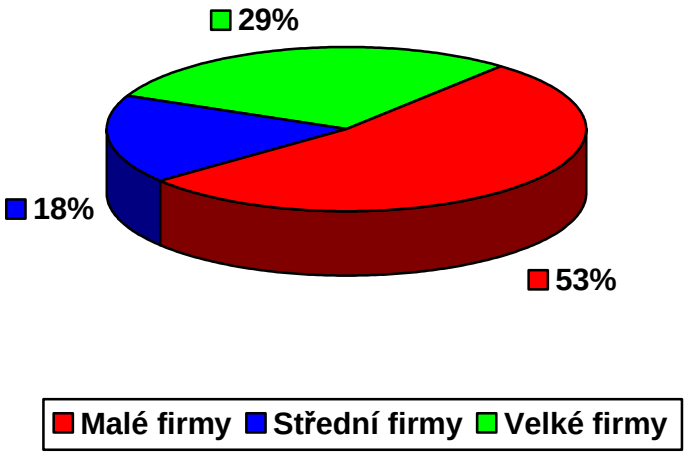
Cílem provedeného průzkumu bylo zjistit podrobnější informace o používání peer to peer aplikací v podnicích. Především jaké aplikace jsou nejvíce používané a jestli jsou si zaměstnanci vědomi možných rizik, které používání peer to peer aplikací obnáší, dále pak jestli podniky nějak omezují nebo přímo zakazují používání těchto aplikací.

Předpokladem tohoto průzkumu je, že především větší firmy budou věnovat této problematice více času a používání peer to peer aplikací budou nějakým způsobem omezovat nebo přímo zakazovat.

Dotazník vznikl na základě konzultací s vedoucím práce panem Ing. Ladislavem Beránkem. Dotazník obsahuje celkem devět otázek a byl navržen tak, aby bylo možné na jednotlivé otázky odpovědět velmi jednoduše, pokud možno vybráním jedné z nabízených možností nebo odpovědět ano/ne a to z důvodů umístění dotazníku na web, konkrétně na http://www.vyplnto.cz. Po té co byl dotazník umístěn na tuto webovou stránku byl rozeslán, kamarádům a kolegům. Dotazník byl vyplněn celkem 17 respondenty.

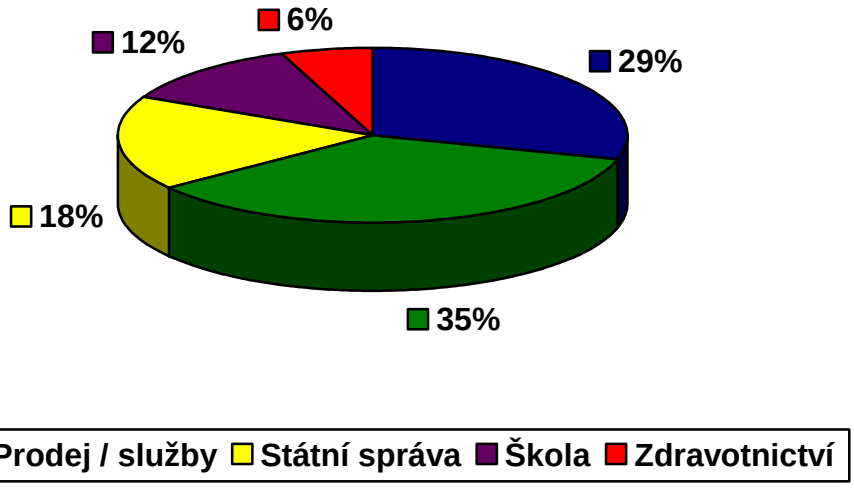
6.2 Výsledky průzkumu

Pro lepší přehled byly organizace rozděleny na tři části podle počtu zaměstnanců. Malé firmy – do 40 zaměstnanců, střední firmy – 40 až 80 zaměstnanců a velké firmy – více než 80 zaměstnanců. Poměr zastoupení firem podle velikostí vidíme na obr. 12.



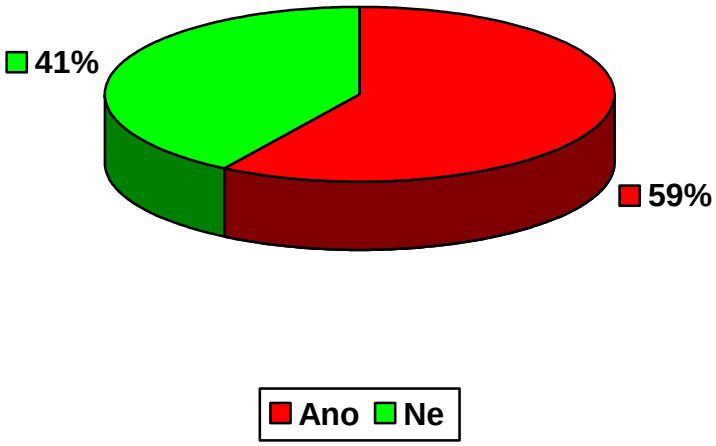
Obr. 12: Zastoupení firem podle velikosti.

Na grafu (obr. 13) je zobrazeno zastoupení firem podle svého oboru.



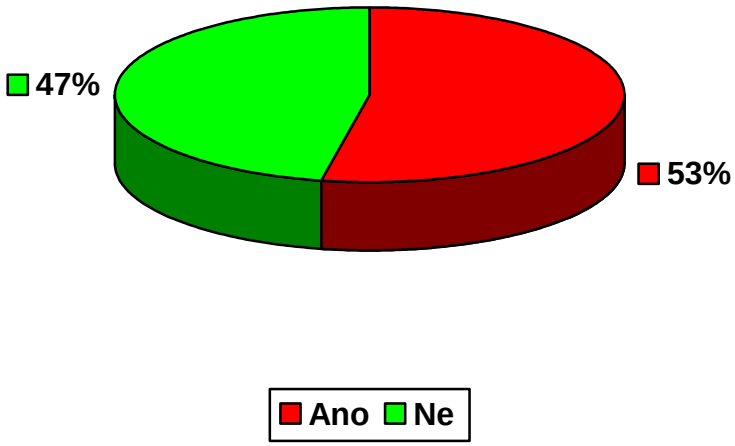
Obr. 13: Zastoupení firem podle oboru.

Na dalším grafu (obr. 14) vidíme kolik firem v procentech přímo zakazuje jakékoli používání peer to peer aplikací. Podle původního předpokladu je to více než polovina firem.

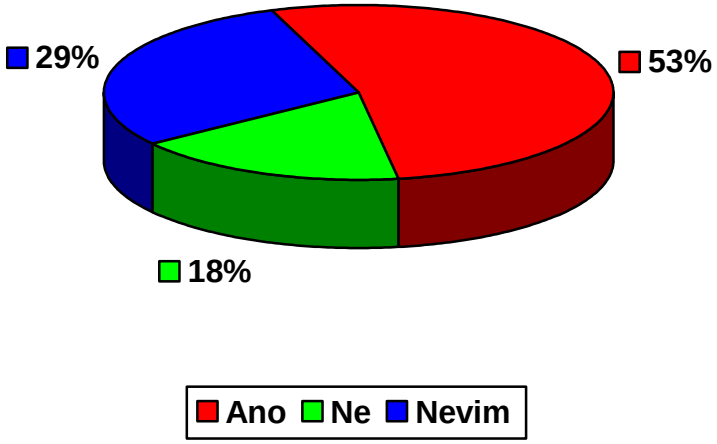


Obr. 14: Zákaz používání peer to peer aplikací ve firmách.

Na následujícím grafu (obr. 15) ovšem vidíme, že víc než polovina respondentů používá peer to peer aplikace i přes přímý zákaz podniků. Tento fakt ukazuje na to, že zaměstnanci jsou špatně informovaní a neuvědomují si jakému nebezpečí vystavují firemní síť, tím že používají peer to peer aplikace. Na grafu (obr. 16) znázorňující kolik respondentů považuje peer to peer aplikace za bezpečnostní hrozbu vidíme, že více než polovina si je vědoma možných rizik, ovšem toto číslo by mělo být pokud možno co nejvyšší.

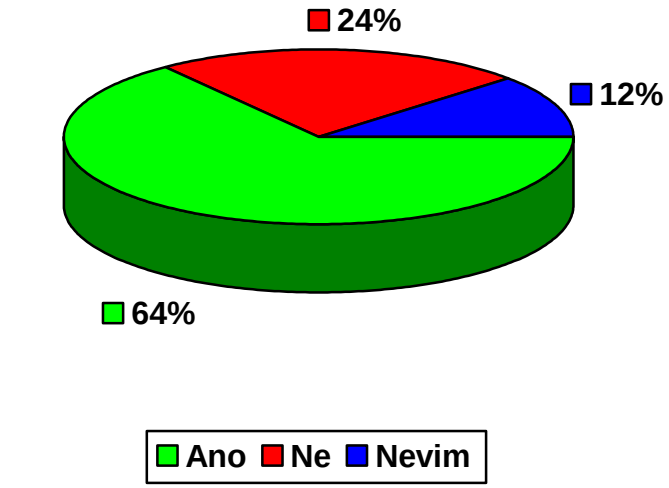


Obr. 15: Používání peer to peer aplikací.



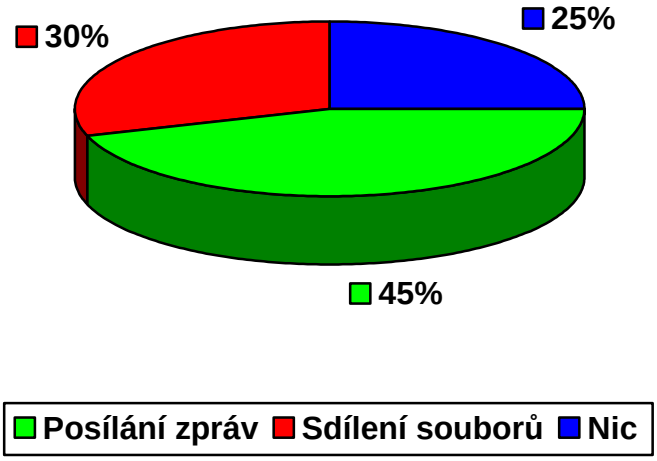
Obr. 16: Peer to peer aplikace jako bezpečnostní hrozba.

Další graf (obr. 17) zobrazuje kolik firem nějakým způsobem omezuje používání peer to peer aplikací (včetně úplného zákazu). Dva respondenti na tuto otázku odpověděli nevím, tento fakt opět ukazuje na to, že firmy nemají dostatečně ošetřenou otázku bezpečnosti v používání peer to peer aplikací.



Obr. 17: Omezení používání peer to peer aplikací.

Další graf (obr. 18) zobrazuje za jakým účelem jsou používané peer to peer aplikace používány.

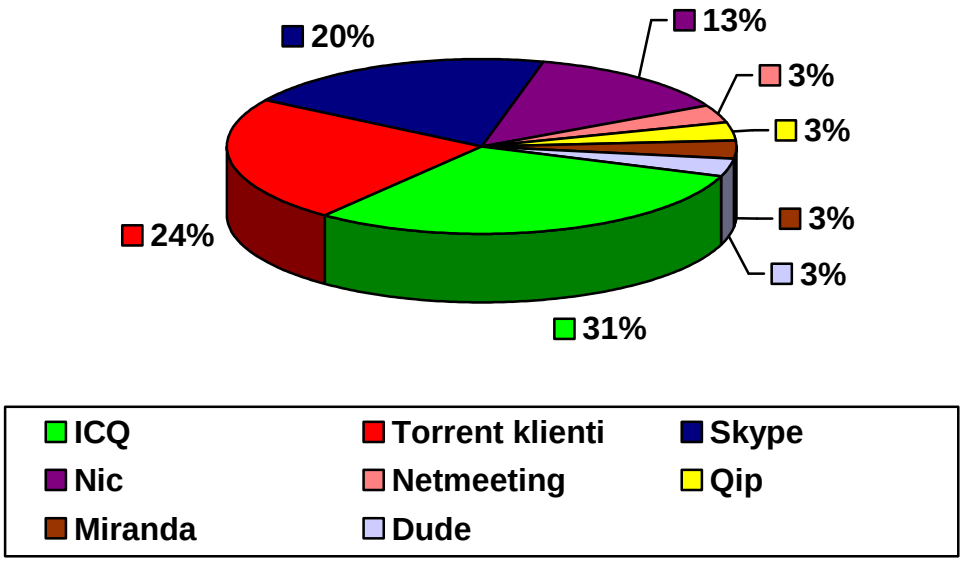


Obr. 18: účel používaných peer to peer aplikací.

Zde vidíme, že peer to peer aplikace jsou nejvíce používány pro komunikaci. Bylo zjištěno, že jedna nejmenovaná firma používá vlastní komunikační program založený na principu peer to peer, který komunikuje jen s uživateli v rámci dané firmy. Nemá tedy přístup za hranice firemní sítě a

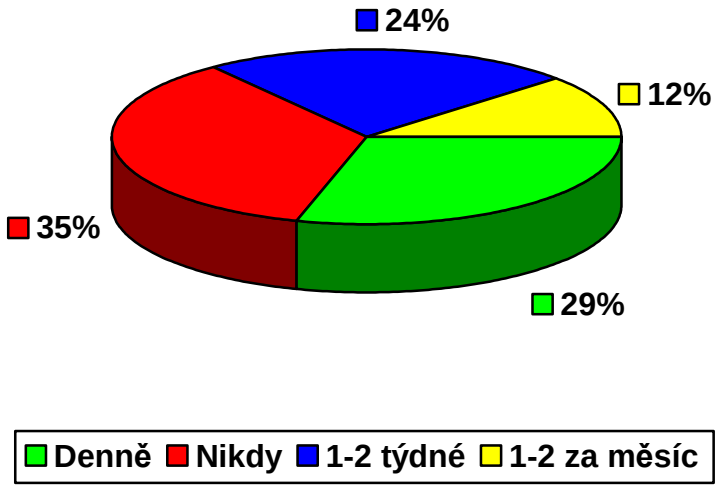
nevystavuje jí tak případným útokům zvenčí. Toto se ovšem týká jen větších firem, které mají prostředky na to vyvinout si vlastní program odpovídající jejich potřebám.

Další graf (obr. 19) zobrazuje konkrétní peer to peer aplikace, které respondenti používají.



Obr. 19: Používané peer to peer aplikace.

Na posledním grafu (obr. 20) je zobrazeno jak často jsou peer to peer aplikace používané. Vidíme zde, že přibližně třetina uživatelů tyto aplikace používá téměř denně, což velmi zvyšuje pravděpodobnost útoků.



Obr. 20: Četnost použití peer to peer aplikací.

Průzkum ukázal, že přibližně polovina respondentů si je vědoma, že používání peer to peer aplikací sebou nese určitá rizika. Ovšem většina zaměstnanců toto přehlíží a i přes zákaz nebo určitá omezení tyto aplikace přesto používá. Mezi nejpoužívanější aplikace patří ICQ, tedy aplikace určená ke komunikaci mezi uživateli. Řešením by tedy bylo dát zaměstnancům adekvátní náhradu, která by ovšem bezpečně fungovala jen v rámci firmy a neohrožovala by tak firemní síť. Dalším řešením je striktně určit pravidla týkající se používání problematických aplikací, pravidelně školit zaměstnance ve správném používání těchto aplikací a informovat je o možných bezpečnostních hrozbách, které byly popsány výše.

Závěr

Není pochyb o tom, že používání peer to peer aplikací sebou nese určitá rizika. Peer to peer aplikace, které byly v této práci testovány obsahují řadu bezpečnostních chyb, které ovšem informovaný uživatel dokáže úplně odstranit nebo hrozící rizika velmi zmírnit. Výsledky testování dokazují, že pokud budeme používat nový operační systém nebo ten starší alespoň pravidelně aktualizovat velkou část závažných bezpečnostních chyb tím úplně odstraníme. Například firma Microsoft si je vědoma bezpečnostních rizik a s těmito problémy se snaží bojovat právě různými opravami svých operačních systémů. Proto je žádoucí, abychom používali operační systém, který je stále podporován svým vydavatelem. Pokud budeme používat starý operační systém, těžko zabráníme možným útokům. Zde se nabízí otázka do jaké míry počítač ohrožují chyby operačního systému nebo na něm spuštěné peer to peer aplikace, ovšem aplikace nelze samostatně otestovat. Také nelze s přesností říci, která z testovaných aplikací je bezpečnější. Aplikace jsou používány už několik let a za tu dobu byly postupně vylepšovány, tudíž rozdíly mezi nimi jsou opravdu nepatrné. Nejméně chyb se však vyskytlo na aplikaci BitTorrent, zejména na systému Windows XP. V současnosti jsou však tyto aplikace pomalu vytlačovány servery určenými pro stahování jakýkoliv dat. Mezi tyto servery patří například rapidshare.com a uloz.to.cz, kde si uživatel může stáhnout téměř cokoliv s minimálním rizikem.

Testování aplikací na systému Linux, také přineslo zajímavé výsledky. Aplikace které byly podrobeny testování neobsahovaly žádné závažné bezpečnostní chyby. Tento fakt lze přisoudit tomu, že Linux je známý pro svoji bezpečnost a proto je také velmi často používán na serverech. Dále pak také skutečnosti, že není tak hojně využíván běžnými uživateli jako systémy od společnosti Microsoft, které tudíž musí čelit většímu počtu útoků. Nicméně pro lepší závěry by bylo vhodné provést testování na více distribucích Linuxu.

Dalším faktorem ovlivňující bezpečnost počítačů nebo firemních sítí je chování samotných uživatelů a zaměstnanců. Nepozorný a neinformovaný uživatel může svým chováním způsobit také velké škody. Proto je velice žádoucí, aby firmy přísně požadovaly dodržování svých bezpečnostních opatření, prováděli školení svých zaměstnanců a také je informovali o nově vznikajících typech útoků a bezpečnostních rizicích.

Literatura

[1] PETERSSON, Linus. *Peer-to-peer time to lock the door*. [s.l.], 2010. 25 s. Blekinge Institute of Technology.

[2] *Jak funguje Peer-to-peer sítě p2p | Direct Connect* [online]. 2009 [cit. 2010-11-20]. Direct Connect. Dostupné z WWW: <http://dc.stahuji.com/direct-connect/jak-funguje-peer-to-peer-site-p2p/>.

[3] KRASEK, Jáchym. *Peer to peer sítě od A do Z: Gnutella a Ares - Lupa.cz* [online]. 2008 [cit. 2010-11-20]. Peer to peer sítě od A do Z: Gnutella a Ares. Dostupné z WWW: <http://www.lupa.cz/clanky/peer-to-peer-site-od-a-do-z-gnutella-a-ares/>.

[4] *Vše o ICQ | PR články | Start.xarea.cz* [online]. 2008 [cit. 2010-11-21]. Start.xarea.cz. Dostupné z WWW: <http://start.xarea.cz/clanek/739481-vse-o-icq/>.

[5] SWISHER, Kara . *Bids are in for AOL* [online]. 2010 [cit. 2010-11-21]. Bids are in for AOL. Dostupné z WWW: <http://news.cnet.com/8301-1023_3-10449039-93.html>.

[6] *SETI@HOME | Projekt Seti@home | Jak to všechno začalo* [online]. 2008 [cit. 2010-11-21]. Projekt Seti@home. Dostupné z WWW: <http://seti.czechnationalteam.cz/s@h/s@h.html>.

[7] BERÁNEK, Ladislav. *Peer-to-peer (P2P) systémy a jejich bezpečnost I.*. České Budějovice, 2010. 3 s. Katedra informatiky, Pedagogická fakulta, Jihočeská univerzita.

[8] BERÁNEK, Ladislav. *Peer-to-peer (P2P) systémy a jejich bezpečnost II.*. České Budějovice, 2010. 4 s. Katedra informatiky, Pedagogická fakulta, Jihočeská univerzita

[9] HALLER, Martin. *Denial of Service (DoS) útoky: úvod - Lupa.cz* [online]. 2006 [cit. 2010-11-25]. Denial of Service (DoS) útoky: úvod.

Dostupné z WWW: <http://www.lupa.cz/clanky/denial-of-service-dos-utoky-uvod/>

[10] Tenable Network Security, Inc. *Nessus 4.2 User Guide*. [s.l.] : [s.n.], 2010. 49 s. Dostupné z WWW: <http://www.nessus.org/documentation/nessus_4.2_user_guide.pdf>.

[11] MIKLE, Ondrej. *Techniky skryté v p2p sieťach - Root.cz* [online]. 2006 [cit. 2010-12-14]. Techniky skryté v p2p sieťach. Dostupné z WWW: <http://www.root.cz/clanky/techniky-skryte-v-p2p-sietach/>.

[12] VACHTL, Pavel. *Sdílení souborů na Internetu a sítě P2P - základní technologický přehled | PC World.cz* [online]. 2009 [cit. 2010-12-14]. PC World. Dostupné z WWW: <http://www.root.cz/clanky/techniky-skryte-v-p2p-sietach/>.

[13] *Referenční model ISO/OSI - přenos dat* [online]. [cit. 2010-12-14]. Referenční model ISO/OSI - přenos dat. Dostupné z WWW: <http://pc-site.owebu.cz/?page=ISO-OSI-2>.

[14] Mrázek Michal. *Torrent, Torrent klienti a Torrent vyhledávače* [online]. 2007 [cit. 2010-12-14]. Referenční model ISO/OSI - přenos dat. Dostupné z WWW: <http://great-webdesign.cz/torrent.phtml