Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Zabezpečení osobního počítače

Jan Cafourek

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Akademický rok 2008/2009

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jan Cafourek

obor Systémové inženýrství

Vedoucí katedry Vám ve smyslu Studijního a zkušebního řádu ČZU v Praze čl. 16 určuje tuto bakalářskou práci.

Název tématu: **Zabezpečení osobního počítače**

Struktura bakalářské práce:

1. Úvod
2. Cíl práce a metodika
3. Hrozby pro počítač v internetu
4. Zabezpečení osobního počítače
5. Výběr vhodného zabezpečovacího softwaru
6. Závěr
7. Seznam literatury
8. Přílohy

Rozsah původní zprávy: 30 - 40 stran

Seznam odborné literatury:

KRÁL, Mojmír: Bezpečnost domácího počítače - prakticky a názorně, Grada Publishing, 2006, ISBN 80-247-1408-6

HORÁK, Jaroslav: Havárie počítače,První pomoc a záchrana, Computer Press, 2006, ISBN 978-80-251-1451-3

ZEMANOVÁ, Petra; RUČKOVÁ, Zuzana a kolektiv: Jak si zachovat zdraví u počítače, Computer Press, 2001, ISBN 8072265466

Vedoucí bakalářské práce: **Ing. Marek Pícka**

Termín odevzdání bakalářské práce: duben 2010

.....
Vedoucí katedry

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

.....
Děkan

V Praze dne: 19.11.2008

Čestné prohlášení

Prohlašuji, že svojí bakalářskou práci „Zabezpečení osobního počítače“ jsem vypracoval samostatně pod vedením svého vedoucího bakalářské práce, za použití odborné literatury zabývající se touto problematikou a dalších informačních zdrojů, které jsou uvedeny v seznamu literatury nebo citacích. Při psaní své bakalářské práce jsem neporušil žádná autorská práva třetích osob.

V Šanově dne ……

Poděkování

Rád bych poděkoval Ing. Marku Píckovi za odborné vedení pří tvorbě mé bakalářské práce, jeho postřehy a cenné rady.

Zabezpečení osobního počítače

Personal computer security

Souhrn

Tato bakalářská práce má v první části za cíl zmapovat a utvořit ucelený informační seznam o zabezpečení osobního počítače. Problematiku zabezpečení nahlíží ze čtyř pohledů: softwarové zabezpečení, fyzické zabezpečení, šifrování dat a bezpečnost z pohledu lidského faktoru. Abychom byli schopni se bránit, musíme znát rizika, která na nás číhají téměř všude, ty jsou v práci také uvedeny. Primárním cílem práce je porovnání a otestování náhodně vybraných firewallu. Pro test jsme vybrali tři softwarové produkty od různých společností. Comodo Internet Security 5.3.175888.1227, Sunbelt Personal Firewall 4.6 a posledním porovnávaným byl Outpost Firewall Pro 2009 6.7.3. Nejlepší firewall jsme určili váženým průměrem, pomocí 4 kriterií (instalace, uživatelské rozhraní, online test a veřejně dostupný test), které byli ohodnoceny podle toho, jak obstáli v testování. Nejlépe si v testu vedl Comodo firewall a zaslouženě skončil na 1. místě, hned za ním byl Outpost firewall a na posledním místě zůstal Sunbelt firewall.

Klíčová slova

Internet, počítačová síť, firewall, Comodo Internet Security, Sunbelt Personal Firewall, Outpost Firewall Pro, šifrování dat, vážený průměr

Summary

This work is in the first part aims to map and create a comprehensive list of information about the security of personal computers. Security issues are viewed from four perspectives: software security, physical security, data encryption and security from the perspective of the human factor. To be able to defend themselves, we need to knouw about the risks that are lurking everywhere. The primary aim is to compare and test a randomly selected firewall. To test we selected three software products from different companies. Comodo Internet Security 5.3.175888.1227, Sunbelt Personal Firewall 4.6 and compared have been the last Outpost Firewall Pro 2009 6.7.3. The best firewall we have determined the weighted average by 4 criteria (installation, user interface, online test and publicly available test), which were rated according to both passed the test. Best in the led the Comodo firewall and deservedly finished on the first place, just behind him was Outpost firewall, and remained last in the Sunbelt firewall.

Keywords

Internet,computer network, firewall, Comodo Internet Security,Sunbelt Personal Firewall, Outpost Firewall, encryption, weighted average

Obsah

Obsah 8

1. Úvod 11

2. Cíl práce a metodika 12

3. Hrozby pro počítač v internetu 13

3.1 Útočníci 13

3.2 Viry 14

3.3 Červy 15

3.4 Trojské koně 15

3.5 Zvláštní případy 16

4. Zabezpečení osobního počítače 19

4.1 Fyzické zabezpečení 20

4.2 Softwarové zabezpečení 21

4.2.1 Antivirové programy 22

4.2.2 Antispyware 24

4.2.3 Firewally 24

4.3 Šifrování dat 24

4.4 Zabezpečení lidského faktoru 25

5. Výběr vhodného zabezpečovacího softwaru 26

5.1 Definice uživatele a kritérií 26

5.2 Firewally 28

5.2.1 Comodo Internet Security 5.3.175888.1227 30

5.2.1.1 Instalace 30

5.2.1.2 Zmapování uživatelského rozhraní 31

5.2.1.3 Online test 32

5.2.1.4 Výsledky veřejného testu 34

5.2.1.5 Shrnutí 35

5.2.2 Outpost Firewall Pro 2009 6.7.3 36

5.2.2.1 Instalace 36

5.2.2.2 Zmapování rozhraní 37

5.2.2.3 Online test 37

5.2.2.4 Výsledky veřejného testu 40

5.2.2.5 Shrnutí 40

5.2.3 Sunbelt Personal Firewall 4.6 41

5.2.3.1 Instalace 41

5.2.3.2 Zmapování rozhraní 42

5.2.3.3 Online test 42

5.2.3.4 Výsledky veřejného testu 45

5.2.3.5 Shrnutí 45

5.3 Přehled výsledků 46

6. Závěr 47

7. Seznam literatury 49

Seznam tabulek

Tabulka 1a Výsledky online testu Comodo……33

Tabulka 1b Výsledky online testu Comodo……34

Tabulka 2 Výsledky veřejně dostupného testu Comodo……35

Tabulka 3a Výsledky online testu Outpost……..38

Tabulka 3b Výsledky online testu Outpost……..39

Tabulka 4 Výsledky veřejně dostupného testu Outpost……40

Tabulka 5a Výsledky online testu Sunbelt……..43

Tabulka 5b Výsledky online testu Sunbelt……..44

Tabulka 6 Výsledky veřejně dostupného testu Outpost……45

Tabulka 7 Výsledky……..46

Seznam obrázků

Obrázek 1 Schéma víceúrovňového zabezpečení……..20

Obrázek 2 Vzorec váženého průměru……28

Obrázek 3 Jak pracuje Firewall……..29

1. Úvod

V dnešní moderní době lidé využívají mnoho užitečných vynálezů, aby si ulehčili svojí práci a čas. Jedním často používaným moderním „pomocníkem“ je i počítač, který umožňuje uživateli dostávat se na internet a pracovat s ním. V současné době je internet využíván ohromnou masou lidí. Někteří ho využívají k práci, jiní jen tak ve volném čase k získávání informací nebo ke komunikaci s přáteli. Někteří lidé si nedovedou představit, že by nebyli jeden den online.

Internet je velmi rozsáhlé prostředí, ve kterém lze bádat a objevovat nové věci. Je to soubor prostředků obsahující propojené servery a směrovače, které spolu dohromady tvoří největší síť na světě. V tomto souboru se vyskytují různé servery, jako jsou třeba webové či poštovní servery. Po připojení do sítě jsou zde k dispozici veškerá data, která Internet obsahuje. Protože se systémy a technologie stále vyvíjí, přináší nám Internet nové a nové možnosti jeho využití. Stále více se rozmáhá internetový obchod, lze zde provozovat bankovnictví, tím pádem se zde uvádí velké množství osobních informací. S jejich používáním roste i míra potřebného zabezpečení, aby nedocházelo k případnému zneužití bez vědomí uživatele.

Zabezpečení internetu není nijak jednoduchá záležitost. Je zde problém velkého počtu uživatelů, s čímž se při jeho zakládání nepočítalo, dalším problémem je, že neexistuje sjednocená organizace, která by zastávala funkci „strážníků“ a zajišťovala by bezpečnost Internetu. K dostatečnému zabezpečení je zapotřebí znát hrozby a rizika, které na nás číhají na veřejných sítích. Aby byl náš počítač dostatečně chráněn, je zapotřebí orientovat se a mít dostatečné informace v této problematice. Dále bezpečnost ovlivňují produkty, které se k zabezpečení využívají. Tato práce by měla popsat softwarové produkty firewall, které se využívají k zabezpečení osobních počítačů.

2. Cíl práce a metodika

Primárním cílem této práce je dospět ke komplexnímu porovnání firewallových produktů a jejich vlastností z hlediska běžného uživatele a určit, který z porovnávaných vyjde nejlépe. Vypracovat ucelený náhled na problematiku zabezpečení osobního počítače. Představit, jak uživatel může zabezpečit svůj přístroj proti zneužití bez jeho vědomí.

V první části práce budu zpracovávat informace zabývající se problematikou zabezpečování počítačů. Informace budu čerpat z odborné literatury a internetových zdrojů o tomto tématu. Deskriptivní metodou budu tvořit ucelený informační soubor, ve kterém bude zaznamenáno, jak lze zabezpečit osobní počítač.

Ve druhé části práce představím vybrané softwarové produkty firewall, budu je porovnávat a zjišťovat jejich klady a zápory. V první řadě se posouzení produktu bude skládat především z náročnosti na obsluhu, celkového ovládání softwaru a přehlednosti uživatelského rozhraní. Tato část bude hodně záviset na mém úsudku, popřípadě muže být doplněna poznatky některých zkušenějších uživatelů pracujících s firewally.

V další fázi porovnávání se na problém zaměřím z pohledu funkčních a bezpečnostních vlastností. Jednotlivé firewally budou v testu nastaveny pro potřeby běžného uživatele a bude zde kladen důraz na bezpečnost. Testování funkčnosti firewallu bude probíhat pomocí online testu. K porovnávání budou zajištěny stejné podmínky a nastavení. Počítač bude mít nastaven operační systém Windows XP, aby se došlo k co nejobjektivnějším výsledkům. K doplnění testu ještě použiji veřejně dostupné výsledky firewall testu. Výsledek porovnávání získáme pomocí váženého průměru. Proto každému kritériu se budou muset přiřadit váhy a hodnoty pro výpočet.

3. Hrozby pro počítač v internetu

Dnešní doba s sebou přináší vyspělou moderní techniku a její čím dál častější využívání. Lidé ji používají téměř ke všemu. Velmi využívaný je i Internet. Lidé ho používají například k nakupování, komunikaci, platebním transakcím a mnoha jiným věcem. Tím pádem koluje na internetové síti velké množství osobních a důvěrných informací. Ty jsou potřeba, aby mohly věci na internetu fungovat. Jsou to např.: přihlašovací jména, hesla, čísla bankovních účtů. Ale mohou to být i informace, které jsou využívány třeba jen k šíření cílené reklamy. Většina lidí je využívá ve svém každodenním životě a to vše v souladu se zákony, které musely být vytvořeny s postupně rozrůstajícími se technologiemi, aby jejich využívání mělo nějaký řád a nebylo informací zneužíváno. Současně s rychlým vývojem technologií, internetu a jeho využití vzrůstá hrozba pro neopatrné uživatele.

Na druhou stranu existují skupiny lidí i jednotlivci, kteří se těmito pravidly neřídí. Vymýšlejí různé způsoby, kterými by osobní informace běžných uživatelů získali. A buď působili škodu jejich jménem či se nezákonně obohacovali na jejich úkor. Snaží se pomocí svých vytvořených nástrojů nabourat do našich počítačů a získat nad nimi kontrolu.

Velkou hrozbou, která na nás na Internetu číhá je počítačová infiltrace. Jde o termín velice rozsáhlý, kterým lze nazvat jakýkoliv neoprávněný vstup do počítačového systému. Nejvíc se do povědomí lidí zapsal pojem „virus“, protože jsou tak označovány všechny typy napadení. Bez ohledu na to, zda se jedná opravdu o virus, červa nebo trojského koně. I když samostatná definice jednotlivých infiltrací bývá složitá, protože jednotlivé typy se mohou prolínat či spolu mutovat, všechny typy infekcí lze označit názvem Malware – MALicious softWARE – škodlivý software.

3.1 Útočníci

Jsou to lidé, kteří se snaží neoprávněně vniknout do našeho počítače za nějakým cíleným účelem. Jejich úmysly bývají záporné a nezákonné. Dělí se na několik skupin:

- *Hacker* – tímto jménem bývají označování všichni „počítačový piráti“, kteří páchají zlo v počítačových sítích. Hacking je snaha dělat věci, ke kterým nemám oprávnění, ale hackeři většinou dále ničeho nezneužívají. Klasický hacker je talentovaný programátor, který vyhledává nedokonalosti v systémech. Tito „praví“ hackeři hledají v informačních systémech problémy a jejich řešení s použitím nových technologií.

- *Skript Kiddies* – je označení pro nezkušené hackery. Ti používají skripty a programy za účelem ohrozit osobní počítače a uživatelské účty. Oběti svých útoků si většinou vybírají skenováním tisíce počítačů a hledají bezbranný cíl. Nezaměřují se na specifický cíl, ale na to co je upoutá a je „otevřeno.“

- *Sniffer* – je program nebo zařízení, které naslouchá síťovému provozu a zachycuje informace běžící po síti. Možnost bránit se před sniffingem muže být v šifrované komunikaci, např. protokolem SSL. Stránky, které komunikují tímto způsobem, využívají hlavně finanční instituce.

- *Lamer* . je slangový výraz pro někoho, kdo vlastně pořádně nerozumí tomu, co dělá. Základ je ze slova lame jako hloupý. Tento útočník používá již dříve napsaný kód nebo dobře zdokumentované exploity k hacknutí, bez toho, aby všemu dobře rozuměl. Pojem lamer se obecně využívá i pro někoho, kdo nechápe, jak věci fungují.

- *Cracker* – je člověk s výbornými znalostmi počítačů, softwarů a programování. Rozdíl mezi crackerem a heckerem je v tom, že cracker získané informace o slabém zabezpečení zneužívá ke kriminálním účelům nebo ve vlastní prospěch. Za crackera může byt také označen ten, kdo se snaží prolomit obrany placeného softwaru proto, aby je mohl využívat bez nutnosti jejich koupě.

3.2 Viry

Jedná se o nejčastější variantu infiltrace. Jejich název vznikl odvozením kvůli jistým podobnostem biologických virů. Virus je schopen sebe-replikace, když je jeho hostitel

připojen. Virus je schopen množení sebe samotného. Hostitelem mohou být například systémové oblasti disku, spustitelné soubory nebo soubory, které nelze vykonat přímo, ale za použití specifických aplikací (word, excel dokumenty). Jakmile je tento hostitel spuštěn, provede se také kód viru. V tomto okamžiku se virus pokouší provést sebe-replikaci a to připojením k dalším vhodným hostitelům. Podle typů hostitele a způsobu infekce lze viry rozdělovat do dalších skupin.

3.3 Červy

Pojmem červ byl prvně označen tzv. Morrisův červ, který v roce 1989 dokázal zahltit velkou část tehdejší sítě, ze které později vznikl Internet. Červy pracují na nižší síťové úrovni nežli klasické viry. Nešíří se pomocí infikovaných souborů, ale za pomoci sítových paketů. Pakety jsou usměrňovány již od úspěšně infikovaného systému na další systémy v internetové síti. Když takový paket dorazí k systému s určitou bezpečnostní dírou, pak může dojít k jeho infekci a následně i k produkci dalších nakažených paketů. Šíření červů je založeno na zneužívání konkrétních bezpečnostních děr operačního systému. Jeho úspěch pak závisí na rozšíření softwaru, který obsahuje zneužitelnou bezpečnostní díru. Protože červi fungují jinak nežli viry, nelze je detekovat pomocí klasického antivirového softwaru.

3.4 Trojské koně

Také se někdy o nich mluví jako o trojanech. Na rozdíl od virů není typ škodlivého kódu schopen sebe-restrikce a infekce souborů. Trojské koně nejčastěji vstupují do počítače pomocí běžných programů, ke kterým jsou připojeny. V současné době se objevují nejčastěji tyto typy trojanů.

- *Password-stealing trojani (PWS)* – typ trojských koňů, který většinou sleduje jednotlivé stisky kláves, ty ukládá a následně i odesílá na dané e-mailové adresy.

- *Destruktivní trojani* – to je klasická forma, jak je klasický trojský kůň chápán. Když je tento typ trojského koně spuštěn, začne likvidovat soubory na disku, nebo ho rovnou kompletně zformátuje.

- *Drozer* – je to takzvaný vypouštěč. Ve svém těle přenáší jiný škodlivý kód (třeba virus), který je následně po aktivaci vypuštěn do operačního systému.

- *Backdoor* – je aplikace typu klient-server. Mají schopnosti hodně podobné s komerčními produkty pro vzdálenou správu počítače. S tím rozdílem, že vystupují anonymně, uživatel není schopen zjistit jejich přítomnost běžným způsobem. To bývá důvodem, proč jsou preventivně antivirové programy detekovány jako jeden z typů infiltrace. Veškerá komunikace probíhá ve většině napadení na bázi TCP/IP, která ve spojení s Internetem umožňuje, aby útočník mohl být vzdálen tisíce kilometrů po celém světě.

3.5 Zvláštní případy

Do této podkapitoly jsou zahrnuta nebezpečí, která nemusí být klasifikována jako infiltrace. Ale přinejmenším jde o nepříjemné záležitosti.

- *Spyware* – je program, který zneužívá Internet k odesílání osobních dat z počítače bez vědomí jeho uživatele. Z počítače jsou odcizována pouze statická data, jako je přehled navštívených stránek či nainstalované programy. Tato činnost bývá prováděna s cílem zjistit zájmy a potřeby uživatele. Informace zjištěné tímto způsobem se využívají pro cílenou reklamu. Ale nikdo zde nedokáže zaručit, že informace nemůže být zneužita. Mnoho uživatelů je také z toho důvodu rozhořčeno legálností spyware. Spyware se šíří společně s řadou běžných programů a jejich autoři o tom vědí.

- *Dealer* – program, který dokáže změnit způsob přístupu na Internet prostřednictvím modemu. Pak místo běžného telefonního čísla pro připojení přesměruje vytáčení na čísla se zvláštním tarifem (až 70 Kč/min). Mnohdy se tak děje zcela nenápadně, zvlášť když uživatel má nastavený nevyhovující Internetový prohlížeč. Dealer využívá nejčastěji soubory typu EXE. Obvykle je do počítače vypuštěn za využití technologie ActiveX, proto mohou nastat problémy uživatelům Internetu Exploreru. Může se jednat i o legální program. Může totiž sloužit jako způsob zpoplatnění

nějaké speciální služby. V dnešní době jsou Dealery už zastaralé a moc se nevyužívají.

- *Adware* – program, který obtěžuje uživatele nevyžádanou reklamou. Hlavními příznaky jsou náhodně vyskakující reklamní okna či samostatná změna domovské stránky webových prohlížečů.

- *Sociální inženýrství* – je založeno na lidské slabosti a důvěřivosti. Představuje způsob průniku do počítače získáním nějakých důležitých údajů.

- *Phishing* – jedná se o podvodnou techniku k získání citlivých údajů (hesla, čísla kreditních karet, apod.) od obětí útočníků. Je založena na principu rozesílání emailových zpráv, které mají představovat oficiální žádost banky či jiné instituce a vyzývají adresáta ke zveřejnění jeho údajů na odkazovou stránku. Tahle stránka může např. napodobovat přihlašovací okno od Internetového bankovnictví. Uživatel zde zadá své přihlašovací jméno a heslo. Tím svoje údaje prozradí útočníkovi, který je pak schopen vykrást peníze z jeho účtu. Tato metoda zkouší, kdy se uživatel nechá nachytat.

- *Pharming* – je útok, specializující se na přesměrování na falešné stránky. Pharming vychází z útoku sociálního inženýrství k získání citlivých informací, kterými nejčastěji bývají uživatelská jména a hesla. Hlavním zájmem útočníků používajících techniku pharmingu se staly e-banking či obchodní hosting e-commerce. Proto je nutné opatřit svůj počítač anti-pharmingem, který nás chrání před vážnou hrozbou. Antivirové a antispyware programy nás neumí ochraňovat před nebezpečím pharmingem.

- *Bot* – říká se mu také web robot, ale spíše se používá jednoduší označení bot. Je to program, který vykonává po celém Internetu jednoduché automatické úkoly. Záškodničtí roboti mohou útočníkovi sloužit ke koordinování a vykonávání automatického útoku na síťové počítače. Např. DoS útok.

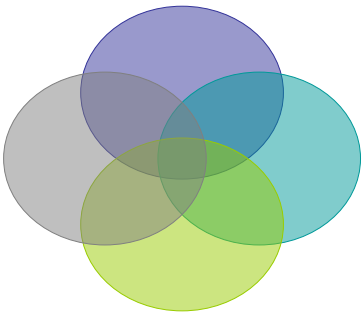
- *DoS útoky* - je to odmítnutí služby. Pokus učinit služby počítače nedostupnými pro uživatele. Častými cíly jsou servery s velkou četností návštěv. DoS útoky mají za cíl přinucení napadeného počítače k resetování nebo spotřebování jeho zdrojů, takže nebude moci nějakou dobu poskytovat určitou službu nebo brzdí komunikaci mezi uživateli. Napadený počítač nemůže nějakou dobu adekvátně komunikovat.

4. Zabezpečení osobního počítače

Stejně tak jako chráníme svoje domovy pomocí dveří, zámků a jiných opatření, je nutné chránit i svůj počítač a v něm uložená data. Podceňování zabezpečení počítače může vést ke ztrátě citlivých dat, ztrátě přihlašovacích jmen a hesel a k následnému zneužití k páchání trestné činnosti vaším jménem či neoprávněnému obohacování. Proto je nutné se orientovat v pravidlech bezpečnosti a rizicích, která na nás číhají na každém „rohu“.

Moderní doba nám přináší automatizaci a výpočetní techniku skoro do všech oblastí lidského života. Je dnes velmi běžné, že počítač je téměř ve všech domácnostech a firmách. Způsob ochrany těchto dvou počítačů bývá odlišný. Jednou z hlavních odlišností je přístup počtu uživatelů k systému. V domácnosti je jednoduché kontrolovat přístup k počítači, protože uživateli jsou jednotliví členové rodiny. Nemusíme tudíž řešit fyzické zabezpečení. Často se v takovýchto případech nepoužívá ani uživatelské jméno a heslo pro přístup do systému pro zjednodušení používání. Ve firmách se ale tato situace výrazně liší (tedy měla by se lišit, jestli má společnost ambice být úspěšná a zůstat na trhu). Přihlašovací hesla jsou zde rutinní záležitostí. Některé firmy mají nadefinovanou délku a skladbu hesel, dokonce i periodu změny. To by se mohlo zdát jako dostatečné zabezpečení. Ovšem opak může být pravdou, pokud nebude PC dostatečně zajištěno z hlediska fyzického zabezpečení.

Bezpečnost osobního počítače závisí na několika faktorech korespondujících se základními oddíly zabezpečení. Ještě před tím, než vůbec začneme řešit nějaké zabezpečení, musíme udělat analýzu rizik. Je pochopitelné, že lákavějším cílem je server s firemními daty, než osobní počítač řadového zaměstnance, ale to neznamená, že budeme chránit jen některé kritické body v systému a zbytek nikoliv. V takovém případě dochází ke klasickému jevu druhu - řetěz je tak pevný, jak pevný je jeho nejslabší článek. Snadno přístupné PC může být pro útočníka vstupenkou.



1. Šifrování dat, 2. Softwarové zabezpečení, 3. Fyzické zabezpečení, 4. Zabezpečení lidského faktoru

Obrázek 1 – Schéma víceúrovňového zabezpečení IT systému.

4.1 Fyzické zabezpečení

Základní myšlenkou tohoto bezpečnostního prvku, je zamezení přístupu nepovolaným osobám k jednotlivým prvkům IT architektury, serveroven, či pracovišť správců systému a tak podobně. Touto cestou můžeme zamezit zcizení nebo poškození hmotného i nehmotného majetku, v neposlední řadě také úniku informací a dat z našich počítačů. Fyzické zabezpečení ale nelze brát jen jako zamezení vstupu do prostor s výpočetní technikou. Proto je nutné na něj pohlížet také jako na celkové fyzické zabezpečení hardwarových a softwarových prvků infrastruktury IT. Zabezpečení z fyzického hlediska se spíše týká firemních počítačů a informačních systému, než počítačů v domácnostech.

Je tedy nezbytné umístění serverů a prvků, které nevyžadují každodenní interaktivní práci s uživateli, do uzamčených prostor s malým pohybem lidí. Serverovny také umožňují efektivně řešit chlazení těchto systémů a problém s jejich záložním zdrojem energie. V neposlední řadě by měl být přesně definován seznam oprávněných osob ke vstupu do těchto prostorů. Přesunem výše uvedených prvků z běžných provozních místností se omezí únik citlivých informací jak ze serverů, tak ze záložních diskových polí.

Útoky se ale také mohou objevovat přes osobní počítač, kde může být podceněn stupeň fyzického zabezpečení. To by se nemělo stávat a ulehčovat tak zlodějům jejich práci. Na první pohled se může zdát, že počítač je v bezpečí - silné heslo do operačního systému, zaheslovaný BIOS proti nechtěným průnikům cizích osob do systému. Je tu však malý problém, kterým je chybějící ochrana PC skříně. Pro útočníka tak není problém otevřít case osobního počítače, vyhledat záložní baterii BIOSu a vyndat ji. Po 30 vteřinách ji zase vrátit a tím dojde k vymazání změn provedených v BIOSu daného počítače a tím i k vymazání hesla do něj. Teď už má útočník skoro vyhráno. Stačí si jen vybrat cestu, kterou se dostane do operačního systému. Pak má plnou kontrolu nad počítačem a nic mu už nebrání v krádeži či manipulaci s daty. Jako první viník bude označena oběť samotná, protože systém v době napadení identifikuje útočníka jako legitimního uživatele. Přitom by jen stačilo udělat několik bezpečnostních opatření. Například uzamknout počítačovou skříň pomocí visacího zámku nebo nainstalovat počítačové skříně do uzamykatelných přihrádek v pracovním stole.

4.2 Softwarové zabezpečení

V každém počítači je nainstalovaný operační systém, který by měl být legálně získaný, a programy, se kterými uživatel pracuje. I přes veškerou snahu jejich tvůrců o maximální zabezpečení, se ve většině případů najdou nějaké bezpečnostní chyby, díky nimž leze např. infikovat počítač nežádoucím softwarem a následně nad ním získat kontrolu nebo získat přístup k osobním datům. Téměř absolutní většina výrobců softwarů poskytuje bezpečnostní aktualizace, které napravují případné vzniklé chyby. Ale nejdůležitější je vlastní přičinění uživatelů. Musí dbát na pravidelné zajišťování aktualizace těchto programů a lépe se tak chránit před riziky napadení nežádoucím softwarem. Mají-li ve svém osobním počítači OS Windows, je dobré mít zapnutou funkci automatické aktualizace. Ta bude uživatele automaticky upozorňovat na dostupnost nových aktualizací a provedení jejich instalace. Pak v podstatě není potřeba se o nic starat, když bude tato šikovná funkce zapnuta. Zapínání se najde v Ovládacích panelech systému Windows.

Je třeba pravidelně aktualizovat své programové vybavení, především pak internetové prohlížeče a jejich doplňky. V případě, že některý program nabízí automatické

aktualizace, je lepší tuhle funkci povolit, aby byla k dispozici neustále nejnovější verze se všemi potřebnými bezpečnostními aktualizacemi.

Každý uživatel počítače by měl mít vytvořený svůj učet, který obsahuje jeho osobní nastavení a osobní data. Většina operačních systémů rozlišuje dva základní typy uživatelů. Jedním z nich je administrátor, který má neomezený přistup k systému. Může instalovat a odebírat programy. Mění a obstarává nastavení a oprávnění pro osobní uživatele. Druhým typem je standardní uživatel, který nemá veškeré kompetence. Pro zachování bezpečnosti je žádoucí, aby při práci uživatel pracoval jako standardní uživatel. Díky tomu dochází ke snížení rizika infikování počítače. Oba dva typy uživatelů by měly být chráněny dostatečně silným heslem, které nelze jednoduše rozluštit a získat tak neomezený přístup k počítači. Pro nastavení uživatelských účtů a jejich hesel je dobré dodržovat určité zásady:

- Každý uživatel PC má svůj vlastní účet zabezpečený silným heslem.
- Heslo k danému účtu by nemělo být jednoduše dostupné, např. napsané vedle počítače.
- Heslo k uživatelským účtům jednotliví uživatelé nesdílejí.
- Pro běžnou práci je lepší pracovat jako standardní uživatel nikoliv jako administrátor.

Dalším důležitým prvkem bezpečnosti je antivirový program. Jeho virová databáze však musí být neustále pravidelně aktualizována. Jen tak se docílí toho, že má program údaje o nejnovějších virech a poskytuje plnohodnotnou ochranu. Viry, červy a jiné nežádoucí softwary jsou dnes nejběžnějším způsobem, jak získat přístup k počítači a citlivým datům.

4.2.1 Antivirové programy

V každém počítači je zapotřebí, dříve než se začnou provádět jakékoliv operace s vnějším okolím, mít nainstalovaný nějaký antivir. Antivirový program kontroluje všechny nejpodstatnější vstupní a výstupní místa, kterými by mohly viry do počítačového

systému proniknout. Viry samotné se mohou definovat jako nežádoucí a ve většině případů škody páchající kódy, které se cíleně šíří.

Antivirový program pracuje na základě virové databáze, která kontroluje data a vyhledává ty s případnou infekcí. Viry se pořád zdokonalují a mění. Dokonce mohou vytvářet také mutace, podobně jako viry přenášející nemoci. Vše probíhá takovou rychlostí, že výrobci antivirových programů musí na tuto situaci reagovat každý den. Proto je virová databáze průběžně aktualizována a je k dispozici uživatelům ke stažení. Stahování z internetu se provádí automaticky. Antivirové programy dnes všechna data, ke kterým máme přístup a pracujeme s nimi, kontrolují na pozadí. Pokud soubory neosahují žádné viry, většinou tuto činnost ani nezaregistrujeme. Samotné antiviry také nabízejí uživatelům, aby zahájili funkci skenování souborů, kdy potřebují nebo chtějí. Dnes už se nekontrolují jen soubory nakopírované z výměnných disků do počítače. Dnešní komplexní řešení musí čelit rozmanitým nástrahám, které bohužel do dnešního světa patří. Nesmíme ale zapomenout, že nestačí jen obezřetný antivirový program, ale obezřetný musí být v první řadě i sám uživatel.

Dělení antivirových programů:

- *On-demand skenery* – to jsou většinou programy využívající rozhraní OS DOS, pro dezinfekci počítače, např.: když operační systém MS Windows není schopen provozu. Bývají většinou součástí antivirového programu.

- *Jednoúčelové antivirové programy* – jedná se o programy, které jsou určeny k detekci, popřípadě i odstranění jednoho konkrétního viru či menší skupiny virů. Tyto specializované antiviry vznikají většinou k likvidaci nějakého viru rozšířeného v dané době.

- *Antivirové systémy* – jedná se o kompletní antivirové řešení, které má za úkol ochraňovat náš počítač před viry a červy šířící se poštou, před škodlivými skripty. Případně zabránit stažení infikovaných souborů do počítače. Komplexní systém může mít ve výbavě firewall a další specializované nástroje.

Na trhu je velké množství nabízených produktů, které nám pomohou zabezpečit osobní počítač. Proto existují antivirová centra, která nám pomohou zorientovat se v široké nabídce antivirových řešení. Existuje i virová databáze, kde lze dohledat informace o určitých virech, abychom věděli, jak se bránit.

4.2.2 Antispyware

Jedná se o podstatnou složku komplexní ochrany počítače. Je to obranný program, který kontroluje všechna data přicházející do počítače, vyhledává škodlivé softwary a znemožňuje přístup čemukoliv, co by mohlo počítač ohrozit. Spyware je program v počítači, který bez vědomí uživatele odesílá data přes internet. Data jsou většinou následně analyzována a zneužita k různým účelům. Např: přístup k citlivým datům, heslům, někdy i cílené reklamy.

4.2.3 Firewally

Ve volném překladu by se dal firewall interpretovat, jako „bezpečnostní brána.“ Dá se říci, že je to software oddělující provoz mezi naší domácí sítí a sítí Internet, přičemž propouští data jedním nebo druhým směrem podle předem nadefinovaných pravidel. Ochraňuje nás hlavně před neoprávněnými průniky do sítě a před odesíláním dat ze sítě bez souhlasu uživatele. V prostředí osobního počítače je instalace firewall brány prvním nejdůležitějším a nejefektivnějším krokem k ochraně počítače.

4.3 Šifrování dat

Šifrování je způsob, jak zabezpečit elektronická data uživatele proti zneužití a tím tak chránit jeho soukromí. Dnes už tento způsob ochrany není záležitostí jen velkých firem a vládních institucí, ale začíná se čím dál tím víc využívat i v jednotlivých domácnostech. Šifrování dat zamezí tomu, že se ke zprávě a datům nedostane další neautorizovaná osoba. Možností jak šifrovat data je několik. Některé šifrovací programy jsou přímo součástí operačního systému. Např.: BitLocker. Tato technologie je k dispozici u OS Windows Vista a Windows 7. Jiné programy lze stáhnout zdarma z internetu, to jsou např. DiskCryptor, FileCryptor či TrueCrypt. Placené šifrovací programy přinášejí uživatelům

lepší funkce. Pro šifrování dat je důležité vybrat cestu - File Encryption nebo Disk Encryption

Disk Encryption je šifrování disku jako jednotného celku. Software, který se pro šifrování disku využívá, šifruje většinou celý pevný disk. Uživatel se pak nemusí starat o to, které soubory by měl zabezpečit nebo jestli náhodou na nějaká data nezapomněl a nenechal je nezabezpečená. Metoda diskového šifrování probíhá průběžně. Tím pak dochází k poklesu výkonu počítače. Efektivně lze data šifrovat pomocí volně dostupného programu TrueCrypt, který umožňuje šifrování diskových oddílů. Používá šifrovací algoritmy, kde lze utvořit až 448-bitový klíč.

File Encryption je cesta šifrování a dešifrování souborů, složek, emailových zpráv a dat odeslaných přes počítačové sítě pomocí k tomu určeného softwaru. Pro šifrování se používá zvolený klíč či heslo k zašifrování určitých souborů. Pro následné otevření takového souboru je vždy potřeba znát klíč. Při šifrování velkého objemu dat může docházet ke zpomalování systému. Dobrá volba pro zabezpečení je také kombinace šifrování a skrytí dat, tím ostatní uživatelé ani nemusí o vašich datech vědět. K zabezpečení souborů a složek se dá využít poměrně hodně rozšířený archivátor WinRAR. Může používat zaheslované RAR archivy, či skrývat obsah. Bez hesla tedy není možno obsah zjistit.

4.4 Zabezpečení lidského faktoru

Je málo pravděpodobné, že jeden člen rodiny bude prodávat informace o druhém. Proto se zabezpečení lidského faktoru tolik nedotýká domácích počítačů. Před problémem lidského faktoru stojí spíše firemní počítače. Proti lidskému faktoru neexistuje žádný bezpečnostní software. Záleží tedy jen na tom, jací lidé budou s počítačem pracovat. Proto by měli být lidé dobře prověřeni už při nástupu do zaměstnání. A podle mého názoru i během činnosti průběžně kontrolováni. Opatrnosti není nikdy dost.

5. Výběr vhodného zabezpečovacího softwaru

V poslední části práce se budu věnovat porovnání náhodně vybraných produktů firewall, kterými jsou Comodo Internet Security, Outpost Firewall Pro 2009, Sunbelt Personal Firewall. Porovnám u nich klady a zápory podle určitých kritérií. Výsledkem bude doporučení jednoho produktu pro našeho uživatele.

5.1 Definice uživatele a kritérií

Uživatel, kterého jsem si vybral pro tuto práci, je uživatel se základními znalostmi o počítačích a komunikačních technologiích. Ví, že existuje Internet, že se na něm sdílí velké množství informací, a že je poslední dobou čím dál tím víc využívaný pro běžné činnosti v každodenním životě pro usnadnění práce a úspory času. Slyšel i o určitých rizicích, které na uživatele číhají při používání počítače na Internetu.

Protože dosud neměl osobní počítač, nemá moc zkušeností se zabezpečením a instalací bezpečnostního softwaru. Vždy využíval jen počítače ve veřejných počítačových kavárnách a tak podobně. Zde počítal s tím, že se nemusí o bezpečnost nijak starat. Nyní ho ale už omrzelo pořád někam chodit, když potřebuje pracovat s počítačem. Rozhodl se tedy pořídit si vlastní počítač, aby mohl být soběstačný a kdykoliv ho využít. Bohužel nevyhledal pomoc odborníků a pořídil si počítač sám. Zakoupil si notebook se slušným výkonem, ve kterém byl nainstalován jen operační systém Windows XP Home edition. Dále si zakoupil antivirový program. V jednom časopise se dočetl, že je dobré mít v počítači aktivní bránu firewall. Bohužel neví, který produkt si má pořídit. Limitující pro něj je špatná znalost anglického jazyka.

Tato práce by mu měla pomoci se zorientovat a vybrat správný produkt. Protože budeme počítat výsledek pomocí váženého průměru, musíme jednotlivým kritériím přiřadit příslušnou váhu (na stupnici 1-5, kdy 5 má nejvyšší váhu). Důležitá kritéria v rozhodování budou.

- *Obtížnost instalace* – jednotlivé firewally budou postupně instalovány do osobního počítače s operačním systémem Windows XP.

  Váha kritéria 3

- *Složitost uživatelského rozhraní* – bude se hodnotit přehlednost, vzhled a funkčnost.

  Váha kritéria 4

- *Internetový test bezpečnosti firewallu* na stránkách Test.bezpečnosti [5] – bude probíhat testování jednotlivých firewallu pomocí online testu. Proběhne základní otestování firewallu a počítače. „*Test je založen na analýze informací o otevřených (a tím pádem napadnutelných) portech síťového rozhraní vašeho počítače nebo firewalu.“*[5] Test ukáže, zda někdo může číst naši poštu, prohlížet náš Internet, dostat se k našim heslům, či k obsahu našeho počítače a tak podobně.

  Váha kritéria 5

- *Veřejně dostupný test* na stránkách Živě – „*Cílem testů je spojit hloubkovou analýzu spolu s jednoduchostí leak testů. Testuje se i pokus o obejití ochrany nebo ukončení běhu firewallu, což je test zaměřený na obranné mechanismy firewallu. Analýza se také zaměřuje na výkonnostní testy a aplikace špionážního softwaru, mezi kterými nalezneme keyloggery a paket sniffery.“* [6]

  Váha kritéria 2

Kritéria budou ohodnocena podle toho, jak si stála v testování na stupnici 1 – 10, kdy desítka je nejlepší. Z ohodnocených kritérií vypočítáme vážený průměr, který bude rozhodující pro konečné porovnávání. Čím vyšší bude průměr, tím lepší bude konečné umístění. Body v hodnocení se budou ubírat za nedostatky odhalené při testování.

$$\bar{x} = \frac{\sum_{i=1}^{n} w_i x_i}{\sum_{i=1}^{n} w_i}$$

Obrázek 2 - Vzorec váženého průměru[11]

W_i – váha kritéria, X_i – hodnota kritéria

5.2 Firewally

Firewall lze brát jako „bezpečnostní bránu.“ Je to softwarové zařízení, které rozděluje provoz mezi dvěma sítěmi, Internetem a domácí sítí, kde propouští jedním nebo druhým směrem data podle určitých předem nadefinovaných podmínek. Firewall nás tedy pak ochraňuje před neoprávněnými průniky ze sítě a odesílání dat z počítače bez toho, aniž by něco uživatel o něčem věděl.

Princip firewallu je takový, že se definují pravidla, podle kterých může probíhat komunikace. Dá se říct, že se povolí služby, které jsou důležité a nutné pro provoz. Ostatní jsou zakázány. Mezi efektivní nástroje, které se využívají, můžeme zařadit SMTP ověřování uživatele nebo IP adresy, kontrolu došlých e-mailů s veřejnými seznamy odesílatelů spamu, prověřování existence domény odesílatele, atd. Firewall nás bude informovat o dění v síti Internetu, které podrobně monitoruje. Bude nás informovat o legálních procesech, vzniklých použitím některé z našich aplikací a dovolí nám tuto činnost uložit jako povolenou nebo zakázanou. Firewall se skládá z několika funkčních skupin.

Paketové filtry bývají často implementovány na routerech. Jsou typické vysokou rychlostí, ale naopak nízkou úrovní zabezpečení, protože jejich úkolem je jen kontrolovat pouze zdrojovou a cílovou adresu a port. Neumí logování událostí ani nedokážou upozornit uživatele na podezřelé aktivity.

Aplikační brány jsou výrazněji zabezpečeny než paketové filtry, ale zase jsou pomalejší a omezují možnosti uživatele. Bývají vymezeny na určitý okruh služeb, které

jsou podporovány. Pro každou další službu je nutné napsat nový tzv. proxi(aplikaci), který bude zajišťovat ochranu před nedůvěryhodnou sítí a kontrolovat všechny pakety pro danou službu.

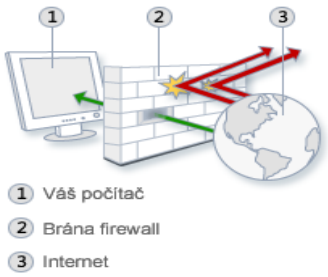
SMLI Gateways má v sobě zahrnuto to nejlepší z předchozích skupin. Rychlost paketových filtrů a zabezpečení aplikačních bran. Provádí své funkce na nejnižší softwarové úrovni, tím může dobře chránit vnitřní síť i sám sebe.

Počítače, které používají operační systém Microsoft Windows mají zabudovanou automaticky bránu Windows Firewall, který má dostupné tři základní nastavení.

- Zapnuto - tento typ nastavení je rozhodně doporučován. Bývá nastaveno jako výchozí. Když je brána Firewall zapnutá, u většiny programů je pak komunikace přes bránu zablokována. Blokování programu se dá zrušit tím, že se program přidá do seznamu vyjímek.

- Blokovat všechna příchozí připojení – tohle nastavení blokuje nevyžádané pokusy o připojení k počítači. Využívá se při potřebě maximální ochraně počítače. Např.: připojení k veřejné síti v hotelu.

- Vypnuto – není doporučeno. Toto nastavení by se nemělo používat. Po vypnutí firewallu bude počítač mnohem méně chráněn před počítačovými zločinci a jejich softwarovými výtvory.



Obrázek 3 – Jak pracuje Firewall [7]

5.2.1 Comodo Internet Security 5.3.175888.1227

Tento program neobsahuje jen samotný Firewall, ale v bezpečnostním balíku je nabízen i antivirus. Je to výtvor z dílny americké firmy Comodo, která se specializuje na vývoj aplikací pro zabezpečení počítačů a sítí. Sleduje aktuální přenos po síti a poskytuje souhrnné statistiky. Zjišťuje, které aplikace komunikují více, než je potřeba. Jeho služby jsou k dispozici zdarma.

5.2.1.1 Instalace

První požadavek, který je potřebný pro instalaci, je volné místo na disku o velikosti 129 MB. Tento požadavek na kapacitu není v dnešní době nijak problematický. V prvním kroku instalace máme možnost zvolit jazyk, ve kterém chceme instalaci softwaru provádět. Protože v instalačním balíčku není obsažen jen firewall, ale i antivirus a GeekBuddy (pomoc s problémy prostřednictvím vzdálené živé podpory). Pro naše testování jsme zvolili instalaci pouze firewallu. V dalším kroku je možnost si nastavit cestu, kam si program nainstalujeme.

Dále dostaneme na výběr rozsah funkcí, které ovlivňují stupeň zabezpečení a také množství zobrazovaných upozornění.

- Jen firewall – tato volba je jen pro ty, kteří potřebují jen síťový firewall
- Firewall s optimální proaktivní ochranou – poskytuje optimální zabezpečení sítě pomocí ochrany proti běžným metodám k překonání firewall.
- Firewall s maximální proaktivní ochranou – nejvyšší stupeň zabezpečení včetně obrany proti úniku informací a malware.

Pro využití běžného laického uživatele jsme zvolili Firewall s optimální proaktivní ochranou, který je v našem případě dostačující.

Potom nás instalace vyzve, zda chceme využívat servery COMODO Secure DNS – to je bezplatná služba pro rychlejší, chytřejší a bezpečnější Internet. V našem případě jsme zvolili souhlas pro využívání této služby. Poté můžeme zahájit instalaci, která trvala jen několik minut. Pak byla potřeba ještě restartovat počítač a instalace byla úspěšně dokončena.

Hodnota kritéria 9

5.2.1.2 Zmapování uživatelského rozhraní

Tento faktor má pro porovnávání velkou váhu, protože se s ním bude uživatel setkávat nejčastěji při používání programu. Po instalaci si firewall automaticky nastaví své funkce. Dále si pak může uživatel nastavit program podle svého. Je možné nastavit si jazyk, kterým s vámi firewall bude komunikovat. Dále vzhled a barvu oken. Obecné nastavení jako jsou automatické aktualizace a podobně jsou samozřejmostí. V další sekci si uživatel může nakonfigurovat bezpečnost a propustnost firewallu. Lze si nastavit, jak často se budou objevovat výsledky a hlášení o činnostech, které probíhají v počítači.

Prostředí je poměrně přehledné a dobře uspořádané. Brzy se v něm uživatel rychle zorientuje a bez problémů s ním může pracovat. Problémem by pro některé uživatele mohlo být skutečnost, že centrum nápovědy není v českém jazyce. Dále musí být uživatel opatrný při odklikávání oken, která se ptají, zda povolit či zakázat aplikaci. Je třeba vše si pozorně pročíst.

Hodnota kritéria 8

5.2.1.3 Online test

Bylo otestováno celkem 19 nejběžnějších služeb. Možnosti vyhodnocení testu jednotlivých služeb byly tři. : A) otevřeno – služba je veřejná v celé síti Internet. Bez vědomí uživatele je to napadnutelné místo. B) odmítnuto – postačí proti napadení, ale neposkytuje dostatečnou ochranu. C) zabezpečeno nebo vypnuto – vyhovující zabezpečení.

Všechny testované služby v bezpečnostním testu dosáhly označení Zabezpečeno nebo vypnuto. Tím test ukázal, že firewall od společnosti Comodo dokáže dobře zabezpečit náš osobní počítač před nebezpečnými vlivy z Internetu.

Port	Služba	Bezpečnostní význam	Stav
21	**FTP**	Veřejný FTP server. Slouží ke kopírování dat. Hackeři jej často používají ke stahování dat a zakódovaných databází hesel.	**Zabezpečeno nebo vypnuto**
23	**Telnet**	Nekódované terminálové spojení --- dá se odposlouchávat. Máte pravděpodobně FIREWALL. Váš správce nechal velkou bezpečnostní díru do systému. Přes terminál se může někdo pokoušet připojit k serveru...	**Zabezpečeno nebo vypnuto**
25	**SMTP pošta**	Služba pro příjem pošty. Pokud je špatně nastavena, umožní z vašeho počítače jednoduše udělat zdroj spamů (nevyžádaných e-mailů). Pokud máte poštovní server bez posledních aktualizací, je zde možnost i server ovládnout!	**Zabezpečeno nebo vypnuto**
80	**WWW server**	Na vašem počítači, popř. serveru, běží veřejný internetový server. Vaše linka do Internetu je sdílena s uživateli vašich stránek. Pokud není webový server dobře nastaven a aktualizován, lze jej napadnout. Je to hackery nejvíc napadaná služba.	**Zabezpečeno nebo vypnuto**
110	**POP3 pošta**	Služba pro stahování pošty. Lze odposlouchávat nebo provést slovníkový útok nebo útok brutální silou, v případě úspěchu má útočník přístup k vaší poště. V případě, že váš účet slouží i ke vzdálenému přístupu k firemní síti, jde o velký bezpečnostní incident.	**Zabezpečeno nebo vypnuto**
135	**RPC Microsoft**	Služba Microsoftu pro volání vzdálených procedur. Hackeři přes ni dokážou například zablokovat počítač.	**Zabezpečeno nebo vypnuto**
137	**NetBIOS Name**	Služba pro sdílení souborů a tiskáren sítě Microsoft. Pokud je otevřena z Internetu, může kdokoliv procházet vaším počítačem.	**Zabezpečeno nebo vypnuto**
139	**NetBIOS Sesion**	Služba pro sdílení souborů a tiskáren sítě Microsoft. Pokud je otevřena z Internetu, může kdokoliv procházet vaším počítačem.	**Zabezpečeno nebo vypnuto**
143	**IMAP Pošta**	Služba poštovního serveru. Popis viz POP3.	**Zabezpečeno nebo vypnuto**

Tabulka č. 1a – výsledky online testu [5]

161	**SNMP**	Protokol SNMP (Simple Network Management Protocol) --- řízení síťových prvků. Může to být také služba běžící pod Windows. Útočník může získat z registru Windows neocenitelné informace, které může dál použít k následným útokům.	**Zabezpečeno nebo vypnuto**
443	**HTTPS WWW**	Kódovaný veřejný WWW server. Je lepší než obyčejný WWW server, nejde odposlouchávat. Může být stále napadnutelný špatnou konfigurací nebo bezpečnostními dírami (Musí se aktualizovat!).	**Zabezpečeno nebo vypnuto**
445	**WIN NT/2000 SMB**	Služba pro sdílení souborů a tiskáren sítě Microsoft. Pokud je otevřena z Internetu, může kdokoliv procházet vaším počítačem nebo získat vaše hesla.	**Zabezpečeno nebo vypnuto**
1080	**SOCKS**	Proxy služba, slouží pro přístup z vnitřní sítě na Internet, přístupná z vnější strany, umožnuje hackerům vydávat se za vás.	**Zabezpečeno nebo vypnuto**
1494	**Citrix**	Služba používaná pro vzdálené ovládání plochy aplikačního serveru.Pokud je služba dostupná pro každého z Internetu, lze na ni provést slovníkový útok nebo útok brutální silou.	**Zabezpečeno nebo vypnuto**
1723	**PPTP tunel**	Vzdálený přístup do podnikové sítě z domácího PC nebo např. laptopu obchodníka, prostřednictvím VPN. Pokud je služba povolena z jakékoli IP adresy, muže provést útočník útok brutální silou nebo slovníkový útok a tím se dostat do firemní sítě.	**Zabezpečeno nebo vypnuto**
3389	**Vzdálená plocha**	Služba pro připojení se k serveru nebo stanici prostřednictvím grafického terminálu. Přes tuto službu je možno pracovat s PC, jako by u něj někdo seděl osobně.	**Zabezpečeno nebo vypnuto**
5900	**VNC server**	Služby používaná pro vzdálené ovládání plochy PC. Spojení je nešifrované, lze odposlochávat --- velmi nebezpečné !	**Zabezpečeno nebo vypnuto**
5000	**UPnP**	Služba pro komunikaci s UPnP (Universal Plug and Play) zařízeními připojenými do vaší sítě	**Zabezpečeno nebo vypnuto**
5631	**PC Anywhere**	Služby používaná pro vzdálené ovládání plochy PC.Pokud je služba dostupná pro každého z Internetu, lze na ni provést slovníkový útok nebo útok brutální silou.	**Zabezpečeno nebo vypnuto**

Tabulka č. 1b – výsledky online testu [5]

Hodnota kritéria 10

5.2.1.4 Výsledky veřejného testu

Ve veřejném testu na stránkách Živě dosáhl produkt Comodo Internet Security velmi slušného výsledku 90% a vysloužil si označení „very good.“

Product		Product score	Level reached	Protection level	Recommendation	Report	Award
	Comodo Internet Security 5.3.176757.1236	100 %	10+	Excellent – 100 %	 GET IT NOW!		

Tabulka č. 2 - hodnoty z testu z internetových stránek Matousek[8]

Hodnota kritéria 9

5.2.1.5 Shrnutí

Po provedení testu a zhodnocení všech kritérií, jsme se dozvěděli, že firewall Comodo Internet Security je produkt, který dostatečně zabezpečí počítač podle požadovaných podmínek.

Instalace proběhla v pořádku a bez problémů. Postupovali jsme podle instrukcí výrobce, kde bylo všechno podrobně popsáno a vysvětleno. Uživatelské rozhraní je komplexně zpracované na dobré úrovni, takže se v něm uživatel snadno po chvilce zorientuje. Lze si nastavit rozhraní podle svého. Například barvu oken a tak podobně. Umožňuje nám také nastavit možnosti, jak nás bude firewall informovat s ohledem na naše potřeby. Čímž nás zbytečně nezatěžuje, když to nepožadujeme. Možnou slabší stránkou je skutečnost, že poradenské centrum není v českém jazyce. Tato skutečnost by mohla způsobit některým uživatelům problémy. V obou testech obstál produkt Comodo na výbornou. Online testování neodhalilo žádnou nezabezpečenou službu. Tento fakt ukazuje na dobrou funkčnost firewallu. Ve veřejném testu obstál velmi dobře. Vysloužil si hodnocení 90% a slovní hodnocení „very good.“ Není žádný vážný důvod proč tento firewall nedoporučit našemu uživateli.

Ø = (9 x 3 + 8 x 4 + 10 x 5 + 9 x 2) : (3 + 4 + 5 + 2) = **9,1** **1.místo**

5.2.2 Outpost Firewall Pro 2009 6.7.3

Firewall nabízí uživateli široké možnosti nastavení, antispywarovou ochranu, automatickou detekci aktualizací. „*Patřičné vyladění pro konkrétní počítač a potřeby uživatele by nemělo dělat problémy ani mírně pokročilým*“.[4]

5.2.2.1 Instalace

Hned po kliknutí na instalaci nás program vyzve k výběru jazyka. Bohužel je v nabídce jen omezené množství jazyků, mezi které čeština nepatří. To může limitovat některé uživatele. Dále se nám v jednom okně stručně produkt představí.

Protože program neobsahuje jen firewall, dostaneme možnost výběru, co chceme instalovat.

- Web Control
- Anti-Spyware protection

Pro náš test jsme zvolili pouze část Web Control. V dalším kroku si navolíme cestu, kam chceme program, který nám zabere na disku 115 MB, nainstalovat. Když nemáme verzi s poslední aktualizací, vyzve nás Outpost Firewall, zda je během instalace chceme stáhnout. Poté můžeme instalaci zahájit. Po nainstalování dostaneme na výběr ze dvou stupňů zabezpečení.

- Advanced – (Pokročilé) – doporučeno pro pokročilé uživatele. Poskytuje vyšší stupeň ochrany proti všem technikám a programům, které jsou používány při obcházení firewallu.
- Normal – doporučuje se ve většině případů. Zajišťuje ochranu proti nejnebezpečnějším technikám pronikání.

Zvolili jsme typ Normal. Už v dalším kroku máme nastavit, zda chceme automatické aktualizace a tak podobně. Poté můžeme instalaci dokončit. Ještě je potřeba restartovat počítač. Po naběhnutí je firewall plně funkční.

Hodnota kritéria 6

5.2.2.2 Zmapování rozhraní

Po zapnutí, pro delší využívání tohoto firewalu, nás program vyzve k registraci. To jsme neprováděli, protože ho máme jen na krátkou dobu pro testování. Uživatelské okno je pěkně zpracované a barevně sladěné do modrobíla. Na levé straně jsou záložky, ze kterých si můžeme vybrat, co zrovna chceme zkontrolovat. Zde jsou jen informační položky o tom, co se děje.

V pravém rohu na horní liště okna je nastavení. Zde si můžeme nastavit vše, co se týče Outpost Firewallu - funkci stupně zabezpečení, detekci útoků, jazyk (zase chybí čeština), kontrolu webu a mnoho užitečného. Další záložkou v pravém rohu je Update, po kliknutí na ni, nám vyskočí okno s informacemi, jaké aktualizace proběhly a kdy.

Hodnota kritéria 6

5.2.2.3 Online test

Bylo otestováno celkem 19 nejběžnějších služeb. Možnosti vyhodnocení testu jednotlivých služeb byly tři. : A) otevřeno – služba je veřejná v celé síti Internet. Bez vědomí uživatele je to napadnutelné místo. B) odmítnuto – postačí proti napadení, ale neposkytuje dostatečnou ochranu. C) zabezpečeno nebo vypnuto – vyhovující zabezpečení.

Outpost firewall v tomto testu dopadl stejně jako předchozí firewall od americké společnosti Comodo. Všechny testované služby byly označeny jako zabezpečeno nebo vypnuto. Z bezpečnostního hlediska není žádný důvod proč ho nedoporučit našemu uživateli. Bez problémů bude plnit svoji funkci ochránce jeho osobního počítače.

Port	Služba	Bezpečnostní význam	Stav
21	**FTP**	Veřejný FTP server. Slouží ke kopírování dat. Hackeři jej často používají ke stahování dat a zakódovaných databází hesel.	**Zabezpečeno nebo vypnuto**
23	**Telnet**	Nekódované terminálové spojení --- dá se odposlouchávat. Máte pravděpodobně FIREWALL. Váš správce nechal velkou bezpečnostní díru do systému. Přes terminál se může někdo pokoušet připojit k serveru...	**Zabezpečeno nebo vypnuto**
25	**SMTP pošta**	Služba pro příjem pošty. Pokud je špatně nastavena, umožní z vašeho počítače jednoduše udělat zdroj spamů (nevyžádaných e-mailů). Pokud máte poštovní server bez posledních aktualizací, je zde možnost i server ovládnout!	**Zabezpečeno nebo vypnuto**
80	**WWW server**	Na vašem počítači, popř. serveru, běží veřejný internetový server. Vaše linka do Internetu je sdílena s uživateli vašich stránek. Pokud není webový server dobře nastaven a aktualizován, lze jej napadnout. Je to hackery nejvíc napadaná služba.	**Zabezpečeno nebo vypnuto**
110	**POP3 pošta**	Služba pro stahování pošty. Lze odposlouchávat nebo provést slovníkový útok nebo útok brutální silou, v případě úspěchu má útočník přístup k vaší poště. V případě, že váš účet slouží i ke vzdálenému přístupu k firemní síti, jde o velký bezpečnostní incident.	**Zabezpečeno nebo vypnuto**
135	**RPC Microsoft**	Služba Microsoftu pro volání vzdálených procedur. Hackeři přes ni dokážou například zablokovat počítač.	**Zabezpečeno nebo vypnuto**
137	**NetBIOS Name**	Služba pro sdílení souborů a tiskáren sítě Microsoft. Pokud je otevřena z Internetu, může kdokoliv procházet vaším počítačem.	**Zabezpečeno nebo vypnuto**
139	**NetBIOS Sesion**	Služba pro sdílení souborů a tiskáren sítě Microsoft. Pokud je otevřena z Internetu, může kdokoliv procházet vaším počítačem.	**Zabezpečeno nebo vypnuto**
143	**IMAP Pošta**	Služba poštovního serveru. Popis viz POP3.	**Zabezpečeno nebo vypnuto**

Tabulka č. 3a – výsledky online testu [5]

161	**SNMP**	Protokol SNMP (Simple Network Management Protocol) --- řízení síťových prvků. Může to být také služba běžící pod Windows. Útočník může získat z registru Windows neocenitelné informace, které může dál použít k následným útokům.	**Zabezpečeno nebo vypnuto**
443	**HTTPS WWW**	Kódovaný veřejný WWW server. Je lepší než obyčejný WWW server, nejde odposlouchávat. Může být stále napadnutelný špatnou konfigurací nebo bezpečnostními dírami (Musí se aktualizovat!).	**Zabezpečeno nebo vypnuto**
445	**WIN NT/2000 SMB**	Služba pro sdílení souborů a tiskáren sítě Microsoft. Pokud je otevřena z Internetu, může kdokoliv procházet vaším počítačem nebo získat vaše hesla.	**Zabezpečeno nebo vypnuto**
1080	**SOCKS**	Proxy služba, slouží pro přístup z vnitřní sítě na Internet, přístupná z vnější strany, umožnuje hackerům vydávat se za vás.	**Zabezpečeno nebo vypnuto**
1494	**Citrix**	Služba používaná pro vzdálené ovládání plochy aplikačního serveru.Pokud je služba dostupná pro každého z Internetu, lze na ni provést slovníkový útok nebo útok brutální silou.	**Zabezpečeno nebo vypnuto**
1723	**PPTP tunel**	Vzdálený přístup do podnikové sítě z domácího PC nebo např. laptopu obchodníka, prostřednictvím VPN. Pokud je služba povolena z jakékoli IP adresy, muže provést útočník útok brutální silou nebo slovníkový útok a tím se dostat do firemní sítě.	**Zabezpečeno nebo vypnuto**
3389	**Vzdálená plocha**	Služba pro připojení se k serveru nebo stanici prostřednictvím grafického terminálu. Přes tuto službu je možno pracovat s PC, jako by u něj někdo seděl osobně.	**Zabezpečeno nebo vypnuto**
5900	**VNC server**	Služby používaná pro vzdálené ovládání plochy PC. Spojení je nešifrované, lze odposlochávat --- velmi nebezpečné !	**Zabezpečeno nebo vypnuto**
5000	**UPnP**	Služba pro komunikaci s UPnP (Universal Plug and Play) zařízeními připojenými do vaší sítě	**Zabezpečeno nebo vypnuto**
5631	**PC Anywhere**	Služby používaná pro vzdálené ovládání plochy PC.Pokud je služba dostupná pro každého z Internetu, lze na ni provést slovníkový útok nebo útok brutální silou.	**Zabezpečeno nebo vypnuto**

Tabulka č. 3b – výsledky online testu [5]

Hodnota kritéria 10

5.2.2.4 Výsledky veřejného testu

Produkt Outpost v testu vystupoval velmi kladně, umístil se na děleném prvním místě společně s produktem Online Armor Personal Firewall. Výsledek testu ukázal hodnotu 93% a označil produkt jako Excellent v zabezpečení osobního počítače.

Product		Product score	Level reached	Protection level	Recommendation	Report	Award
	Outpost Security Suite Pro 7.0.1.3376.514.1234.401	97 %	10+	Excellent	GET IT NOW!		

Tabulka č. 4 - hodnoty z testu z internetových stránek Matousek[8]

Hodnota kritéria 10

5.2.2.5 Shrnutí

Nainstalovat tento bezpečnostní software nevyžadovalo žádnou nadprůměrnou znalost počítačů. Byla trošku zdlouhavější, ale nenastal nikde žádný problém. Slabou stránkou je, že instalaci nelze provádět v češtině. I pak celý firewall s uživatelem komunikuje v cizím jazyce. Uživatelské rozhraní je rozpracované celkem dobře a přehledně. Není problém si firewall přizpůsobit podle svých potřeb. Online test dopadl stejně jako u Comodo firewallu. Všechny testované služby jsou zabezpečeny proti internetovým rizikům. Ve veřejně dostupném testu se Outpost firewall blýsknul v nejlepším možném světle. Obsadil první příčku z testovaných a vysloužil si ohodnocení Excellent. V testu dosáhnul 93%.

Jeho funkčnost z hlediska bezpečnosti je precizní. Bezpečně se postará o váš počítač, tak že uživatel se může bezstarostně pohybovat po internetu. Jediné co ho řadí za Comodo firewall je, že někteří uživatelé budou postrádat komunikaci v našem mateřském jazyce.

Ø = (6 x 3 + 6 x 4 + 10 x 5 + 10 x 2) : (3 + 4 + 5 + 2) = **8** **2.místo**

5.2.3 Sunbelt Personal Firewall 4.6

Tento Firewall je k dispozici jako freeware s osekanými funkcemi. Plnou verzi si musí uživatel uhradit. Výhodou plné verze je především vzdálená správa či zaheslování nastavení nebo blokování skriptů. Ale i v bezplatné verzi nalezneme vše potřebné pro ochranu našeho počítače a filtrování dat. Všechny funkce nám však budou k dispozici na vyzkoušení po 30 dnů.

5.2.3.1 Instalace

Po poklepání na instalační ikonu musíme chvíli počkat. Vyskočí totiž okno - Příprava na instalaci. V prvním kroku musíme pro pokračování souhlasit s licenčními pravidly společnosti. Sunbelt nám nabídne cestu, kam nám chce program nainstalovat. Samozřejmě je možnost tuto cestu zadat ručně. Následně dostaneme na výběr ze dvou možností nastavení firewalu.

- Simple (jednoduché) – jedná se o typické nastavení pro většinu uživatelů. V tomto výchozím nastavení se vás firewall nebude na nic ptát. Později je pak možnost přepnout na rozšířený režim.

- Advanced (pokročile) – toto nastavení zajišťuje vyšší bezpečnost a flexibilitu pro pokročilé uživatele. Firewall se vás bude ptát na dosud neznámé síťové komunikace.

Protože testujeme firewally pro začínajícího uživatele, zvolili jsme variantu Simple. Potom můžeme zahájit instalaci. Instalace probíhala pouze v anglickém jazyku. Po dokončení byla ještě potřeba restartovat počítač. Když operační systém opět naběhl, nabídl nám Sunbelt stažení nových aktualizací.

Hodnota kritéria 6

5.2.3.2 Zmapování rozhraní

Po spuštění uživatelského okna na nás čekalo velké překvapení. Protože instalace probíhala v angličtině a nebyla ani možnost výběru jazyka, bylo velkým překvapením, že s námi firewall komunikoval v češtině.

Uživatelské rozhraní je celkem jednoduše, ale efektivně zpracované. Na úvodní straně jsme informováni o tom, co se v počítači zrovna děje, co je spuštěno, co připojeno. Je tu graficky zpracován pohyb dat z počítače i do počítače. Na levé straně je sloupeček se záložkami, kde si můžeme vybrat z toho, co zrovna chceme zjistit, či nastavit. Uživatelské prostředí je zpracované jednoduše a na první pohled s kombinací odstínů modré barvy vypadá trochu stroze. Na druhou stranu je přehledné a uživatele zbytečně nerozptyluje a nezatěžuje.

Hodnota kritéria 8

5.2.3.3 Online test

Bylo otestováno celkem 19 nejběžnějších služeb. Možnosti vyhodnocení testu jednotlivých služeb byly tři. : A) otevřeno – služba je veřejná v celé síti Internet. Bez vědomí uživatele je to napadnutelné místo. B) odmítnuto – postačí proti napadení, ale neposkytuje dostatečnou ochranu. C) zabezpečeno nebo vypnuto – vyhovující zabezpečení.

I v tomto testu nevyšla žádná služba nezabezpečená, takže firewall plní svojí úlohu správně.

Port	Služba	Bezpečnostní význam	Stav
21	**FTP**	Veřejný FTP server. Slouží ke kopírování dat. Hackeři jej často používají ke stahování dat a zakódovaných databází hesel.	**Zabezpečeno nebo vypnuto**
23	**Telnet**	Nekódované terminálové spojení --- dá se odposlouchávat. Máte pravděpodobně FIREWALL. Váš správce nechal velkou bezpečnostní díru do systému. Přes terminál se může někdo pokoušet připojit k serveru...	**Zabezpečeno nebo vypnuto**
25	**SMTP pošta**	Služba pro příjem pošty. Pokud je špatně nastavena, umožní z vašeho počítače jednoduše udělat zdroj spamů (nevyžádaných e-mailů). Pokud máte poštovní server bez posledních aktualizací, je zde možnost i server ovládnout!	**Zabezpečeno nebo vypnuto**
80	**WWW server**	Na vašem počítači, popř. serveru, běží veřejný internetový server. Vaše linka do Internetu je sdílena s uživateli vašich stránek. Pokud není webový server dobře nastaven a aktualizován, lze jej napadnout. Je to hackery nejvíc napadaná služba.	**Zabezpečeno nebo vypnuto**
110	**POP3 pošta**	Služba pro stahování pošty. Lze odposlouchávat nebo provést slovníkový útok nebo útok brutální silou, v případě úspěchu má útočník přístup k vaší poště. V případě, že váš účet slouží i ke vzdálenému přístupu k firemní síti, jde o velký bezpečnostní incident.	**Zabezpečeno nebo vypnuto**
135	**RPC Microsoft**	Služba Microsoftu pro volání vzdálených procedur. Hackeři přes ni dokážou například zablokovat počítač.	**Zabezpečeno nebo vypnuto**
137	**NetBIOS Name**	Služba pro sdílení souborů a tiskáren sítě Microsoft. Pokud je otevřena z Internetu, může kdokoliv procházet vaším počítačem.	**Zabezpečeno nebo vypnuto**
139	**NetBIOS Sesion**	Služba pro sdílení souborů a tiskáren sítě Microsoft. Pokud je otevřena z Internetu, může kdokoliv procházet vaším počítačem.	**Zabezpečeno nebo vypnuto**
143	**IMAP Pošta**	Služba poštovního serveru. Popis viz POP3.	**Zabezpečeno nebo vypnuto**

Tabulka č. 5a – výsledky online testu [5]

161	**SNMP**	Protokol SNMP (Simple Network Management Protocol) --- řízení síťových prvků. Může to být také služba běžící pod Windows. Útočník může získat z registru Windows neocenitelné informace, které může dál použít k následným útokům.	**Zabezpečeno nebo vypnuto**
443	**HTTPS WWW**	Kódovaný veřejný WWW server. Je lepší než obyčejný WWW server, nejde odposlouchávat. Může být stále napadnutelný špatnou konfigurací nebo bezpečnostními dírami (Musí se aktualizovat!).	**Zabezpečeno nebo vypnuto**
445	**WIN NT/2000 SMB**	Služba pro sdílení souborů a tiskáren sítě Microsoft. Pokud je otevřena z Internetu, může kdokoliv procházet vaším počítačem nebo získat vaše hesla.	**Zabezpečeno nebo vypnuto**
1080	**SOCKS**	Proxy služba, slouží pro přístup z vnitřní sítě na Internet, přístupná z vnější strany, umožnuje hackerům vydávat se za vás.	**Zabezpečeno nebo vypnuto**
1494	**Citrix**	Služba používaná pro vzdálené ovládání plochy aplikačního serveru.Pokud je služba dostupná pro každého z Internetu, lze na ni provést slovníkový útok nebo útok brutální silou.	**Zabezpečeno nebo vypnuto**
1723	**PPTP tunel**	Vzdálený přístup do podnikové sítě z domácího PC nebo např. laptopu obchodníka, prostřednictvím VPN. Pokud je služba povolena z jakékoli IP adresy, muže provést útočník útok brutální silou nebo slovníkový útok a tím se dostat do firemní sítě.	**Zabezpečeno nebo vypnuto**
3389	**Vzdálená plocha**	Služba pro připojení se k serveru nebo stanici prostřednictvím grafického terminálu. Přes tuto službu je možno pracovat s PC, jako by u něj někdo seděl osobně.	**Zabezpečeno nebo vypnuto**
5900	**VNC server**	Služby používaná pro vzdálené ovládání plochy PC. Spojení je nešifrované, lze odposlochávat --- velmi nebezpečné !	**Zabezpečeno nebo vypnuto**
5000	**UPnP**	Služba pro komunikaci s UPnP (Universal Plug and Play) zařízeními připojenými do vaší sítě	**Zabezpečeno nebo vypnuto**
5631	**PC Anywhere**	Služby používaná pro vzdálené ovládání plochy PC.Pokud je služba dostupná pro každého z Internetu, lze na ni provést slovníkový útok nebo útok brutální silou.	**Zabezpečeno nebo vypnuto**

Tabulka č. 5b – výsledky online testu [5]

Hodnota kritéria 10

5.2.3.4 Výsledky veřejného testu

U nás nejvyužívanější firewall v testu nás moc neuspokojil. Výsledné hodnoty se zastavili na 5% a tím si nevysloužil ani žádné slovní hodnocení. V testu se dělí o poslední příčky pořadí.

Product		Product score	Level reached	Protection level	Recommendation	Report	Award
	Sunbelt Personal Firewall 4.6.1861.0	3 %	1	None	Not recommended		–

Tabulka č. 6 - hodnoty z testu z internetových stránek Matousek[8]

Hodnota kritéria 3

5.2.3.5 Shrnutí

Poslední testovaný firewall od značky Sunbelt z pohledu zabezpečení osobního počítače dopadl dobře. V online testu neukázal žádnou napadnutelnou mezeru. Všechny služby byly vyhodnoceny jako zabezpečeny. Bohužel ve veřejném testu se propadl na poslední příčky v hodnocení. Dosáhl pouze 5% (na rozdíl od dalších dvou porovnávaných, ty měly přes 90%), tenhle špatný výsledek si nezasloužil ani žádné sloní hodnocení.

Na druhou stranu uživatelské prostředí je přehledně zpracované a nemusel by mít s ovládáním problém ani začátečník. Sice působí stroze, ale svojí funkci splňuje. Na rozdíl od instalace je zpracováno v českém jazyce. I když instalace není nijak těžká a proběhla snadno a v pořádku. Uživatelé bez znalosti angličtiny s ní budou mít problémy.

Ø = (6 x 3 + 8 x 4 + 10 x 5 + 3 x 2) : (3 + 4 + 5 + 2) = **7,6** **3.místo**

5.3 Přehled výsledků

Po otestování všech testovacích kritérií a výpočtu váženého průměru jsme dospěli k výsledkům v následující tabulce.

Firewall	Instalace	Uživatelské rozhraní	Online test	Veřejný test	Vážený průměr	**Konečné pořadí**
Comodo	9	8	10	9	9,1	1.
Outpost	6	6	10	10	8	2.
Sunbelt	6	8	10	3	7,6	3.

Tabulka č.7 - Výsledky

6. Závěr

Cílem práce bylo vytvořit ucelený náhled na zabezpečení osobního počítače a nastínit rizika, která na nás číhají na Internetu. Dalším přínosem bylo porovnání vybraných firewallů podle určených kritérií. Na základě tohoto srovnání jsme doporučili nejlepší software našemu uživateli.

V první části práce jsme zmapovali možnosti zabezpečení osobního počítače ze čtyř pohledů - šifrování dat, softwarové zabezpečení, fyzické zabezpečení a zabezpečení lidského faktoru. Ty by se měly všechny dodržovat, aby byla zajištěna maximální ochrana počítače a dat, která v sobě nese, proti zneužití bez vědomí uživatele. Ještě v této části byla nastíněna možná rizika a útoky, které mohou být prováděny na náš počítač za účelem získání citlivých dat uživatele a jejich následné zneužití.

Ve druhé části jsme si určili imaginárního uživatele začátečníka, pro kterého jsme měli vybrat nejvýhodnější firewall podle předem určených kritérií. Porovnávací kritéria pro náš test byla obtížnost instalace, přehlednost uživatelského rozhraní, výsledky online testu a výsledky veřejného testu. Pro porovnání jsme náhodně vybrali tři firewally od různých výrobců. Sunbelt Personal Firewall 4.6, Outpost Firewall Pro 2009 6.7.3, Comodo Internet Security 5.3.175888.1227. Každý z testovaných produktů jsme nainstalovali, zmapovali uživatelské rozhraní a následně otestovali, ohodnotili kritéria a vypočítali vážený průměr. Nejlépe z testovaných dopadl Comodo firewall, na druhém místě skončil Outpost firewall a na třetím místě se umístil firewall Sunbelt.

Prvním z testovaných firewallu byl od společnosti Comodo. Tento firewall se v testu umístil nejlépe. Vážený průměr měl hodnotu 9,1. Jeho instalace probíhala velmi snadno podle instrukcí v každém kroku. Jako jediný nám umožnil vést instalaci v češtině. Uživatelské rozhraní bylo přehledné a funkční. Uživatel si ho mohl nastavit podle svého uvážení. Při obou testech si firewall vedl dobře. V online testu všechny testované služby byly označeny jako zabezpečené. Ve výsledcích veřejného testu získal 90%.

Outpost firewall si v testování nevedl také vůbec špatně. Jedinou jeho nevýhodou bylo, že nepodporuje český jazyk a to by limitovalo našeho uživatele. Jinak z pohledu

funkčnosti jsou s Comodo firewallem srovnatelné. Instalace byla celá v angličtině, ale nebyla nijak složitá. Uživatelské rozhraní je hezky upravené, laděné do modrobílé barvy. Online test přinesl výsledek zabezpečení všech testovaných služeb. Ve veřejném testu dopadl ze všech nejlépe. Dostal 93% a umístil se v něm na prvním místě. Vážený průměr měl hodnotu 8 a celkově skončil na 2.místě.

Poslední test prověřil produkt Sunbelt firewall. Získal v testu vážený průměr 7,6 a zůstal na třetím místě. Instalace probíhala opět v angličtině, ani nebyla možnost výběru jazyka. Pak nás ale firewall překvapil, když v uživatelském rozhraní s námi komunikoval v češtině. Rozhraní je dobře zpracováno. Působí sice trochu stroze, ale jeho funkčnost je výborná. V online testu dopadl jako všechny ostatní, ale ve výsledcích veřejného testu hodně zaostával. Dostal v něm jen 5% a řadil se mezi nejhorší produkty.

Takže vítězem našeho testu je Comodo firewall a proto ho doporučujeme našemu uživateli jako nejvhodnější produkt pro instalaci do jeho osobního počítače.

7. Seznam literatury

[1] HORÁK, Jaroslav: Havárie počítače, První pomoc a záchrana, Computer Press, 2006, ISBN 978-80-251-1451-3

[2] STREBE, Matthew. Firewally a proxy-servery: Praktický průvodce. Brno: Computer Press. ISBN 80-7226-983-6

[3] Mojmír Král Bezpečnost domácího počítače – prakticky a názorně, Grada Publishing a.s., ISBN 80-247-1408-6

[4] ZEMANOVÁ, Petra; RUČKOVÁ, Zuzana a kolektiv: Jak si zachovat zdraví u počítače, Computer Press, 2001, ISBN 8072265466

[5]Test bezpečnosti [online]. 2011 [cit. 2011-2-17]. Test dostupný z WWW: http://test.bezpecnosti.cz/

[6] Živě [online]. 2011 [cit. 2011-2-18]. Veřejný test dostupný z WWW: http://www.zive.cz/bleskovky/nove-testy-firewallu-outpost-vede-sunbelt-a-zone-alarm-se-propadaji/sc-4-a-145759/default.aspx

[7] obrázek [online]. 2011 [cit.2011-2-22] dostupný na WWW: http://windows.microsoft.com/cs-CZ/windows-vista/What-is-a-firewall

[8] Internetový zdroj Matousec dostupný na WWW: http://www.matousec.com/

[9]Bezpečný internet dostupný na WWW: http://www.bezpecnyinternet.cz/zacatecnik/zabezpeceni-pocitace/default.aspx/

[10] Internetový zdroj dostupný na WWW: http://www.securityrevue.com/article/2010/09/vyznam-fyzickeho-zabezpeceni-it-systemu/

[11] Vzorec [online]. 2011 [cit.2011-3-16] dostupný na WWW:

http://cs.wikipedia.org/wiki/V%C3%A1%C5%BEen%C3%BD_pr%C5%AFm%C4%9Br