ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

DIPLOMOVÁ PRÁCE

2010 **Tomáš Kořenek**

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Zabezpečení a monitoring lokální sítě" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 6. 4. 2010 _____

Poděkování

Tímto děkuji panu Ing. Martinu Havránkovi za odborné vedení a připomínky k diplomové práci. Zároveň děkuji firmě Crazy Tomato s.r.o a Petru Zeisbergerovi za ochotu při poskytování potřebných podkladů a konzultace.

Souhrn

Tato práce se věnuje neustále opomíjenému odvětví, kterým je zabezpečení a monitoring lokální sítě. Bezproblémová funkčnost lokální sítě je jedním ze základních předpokladů pro dostupnost určitých klíčových služeb potřebných pro jakoukoliv firmu.

V teoretické části práce budou shrnuty dostupné prostředky, které v současné době slouží k zabezpečení lokální sítě. Tyto prostředky budou rozděleny jako hardwarové a softwarové vzhledem k jejich odlišným specifikacím a funkcím. V hardwarové části bude probrána infrastruktura, UPS, 802.1X či síťové prvky s integrovanou ochranou. V softwarové části bude analyzována důležitost uživatelských práv, bezpečnost hesel, antivirové programy, firewally, DMZ či IDS/IPS/IDPS.

Zabezpečení Wi-Fi sítí patří do lehce odlišné problematiky a bude probráno v samostatné kapitole. V závěrečné části literární rešerše budou presentována dostupná řešení pro monitoring a správu lokální sítě.

Cílem této práce bude sestavení optimální konfigurace pro zabezpečení a monitoring lokální sítě, která bude vytvořena na základě získaných znalostí v teoretické části. Tato optimální bezpečnostní konfigurace bude přímo porovnána s bezpečnostní situací ve vybrané firmě. Pokud bude situace ve vybrané firmě vykazovat nedostatky v zabezpečení, budou na základě optimální konfigurace vyvozena doporučení pro zlepšení. Tato doporučení budou ve výsledku prezentována v určitém pořadí, které bude dáno bezpečnostním rizikem a cenou daného doporučení.

Klíčová slova

lokální síť
monitoring
zabezpečení lokální sítě
firewall
IDS IPS IDPS
zabezpečení Wi-Fi

Summary

This work will discourse the very often overlooked branch which is security and monitoring of local network. Perfectly functioning local network is one of the key factors for availability of some of the important services required by given company.

The theoretical part will be divided into 4 chapters. First two chapters will analyze the hardware and software devices that are used for securing the local network. Hardware devices are for example UPS, 802.1X and routers with integrated security components etc. Software part will discuss user groups, passwords, anti-virus, firewall, DMZ and IDS/IPS/IDPS.

The security of Wi-Fi network wil be discussed in separate chapter due to its importance. The last theoretical chapter will list some of the most popular tools for monitoring of the local network.

Aim of the of the practical part will the optimal security configuration which will be based on facts gained from the theoretical part. This optimal configuration will be directly compared to configuration of chosen company. If this comparison will reveal any weak points then possible recommendations will be pointed out. Economical analysis and repayment time of any possible future investments will be part of recommendations.

Key words

local network
monitoring
securing of local network
firewall
IDS IPS IDPS
securing of Wi-Fi

1 Úvod

Jakákoliv firemní lokální síť představuje jeden ze základních předpokladů pro práci každého zaměstnance. Většina firem v dnešní době spoléhá na e-mailovou komunikaci a internet, což jsou služby, jejichž sdílení umožňuje lokální síť spolu s mnoha dalšími funkcemi. Samotná síť je složitý celek a je tedy zřejmé, že komplexní zabezpečení může často představovat velký problém. Dobře zabezpečená a fungující lokální síť by měla být standardem, ale bohužel tomu tak ve většině firem není. V současnosti je např. zhruba 60% firemních Wi-Fi sítí zabezpečeno velmi slabě nebo dokonce vůbec. Nefunkční lokální síť může znamenat pozastavení výrobního procesu nebo neschopnost firmy správně fungovat. Ztráta klíčových dat může firmu připravit o konkurenční výhodu nebo znevýhodnit pozici firmy na trhu.

Dobře zabezpečená lokální síť by měla poskytovat potřebné služby a zároveň by měla být zajištěna, tak aby firemní data nemohla být ohrožena cizím útočníkem, havárií komponenty, nebo prostě zásahem neopatrného zaměstnance. K vytváření a správě lokálních sítí se používá obrovské množství komerčních produktů. Většina malých firem bohužel disponuje velmi omezeným rozpočtem pro zabezpečení či rozšiřování informačních a komunikačních technologií. Bezpečnostní politika v takovýchto firmách vychází z předpokladu, že pokud dané zařízení či komponenta funguje, tak není důvod investovat do lepšího zabezpečení. Je mnohdy téměř nemožné nalézt v omezeném rozpočtu takovou konfiguraci, která by poskytla alespoň dostatečné zabezpečení v celém rizikovém spektru.

Částečným řešením tohoto problému mohou být volně šiřitelné programy, které ve vhodné kombinaci představují téměř srovnatelnou úroveň zabezpečení jako produkty komerční. Může však také nastat neřešitelná situace a firma musí podstoupit kompromisy, které přímo povedou k oslabení struktury celé sítě.

Hledání pomyslného bezpečnostního i finančního optima pro konfiguraci dané lokální sítě představuje problém, který lze řešit logickým plánováním a pečlivým vybíráním produktů a jejich eventuelních kombinací.

2 Cíl práce a metodika

V literární části této práce budou shrnuty v současnosti dostupné prostředky používané k zabezpečení a monitorování lokální firemní sítě. Na základě tohoto shrnutí bude vytvořena optimální konfigurace pro obecný IT profil malé či střední firmy.

Cílem práce je vytvoření optimální konfigurace, která může sloužit i jako vzor pro další eventuelní bezpečnostní analýzy. Cílem tedy není sestavení nejlepší možné konfigurace, ale takové konfigurace, která dostatečně zabezpečí lokální síť firmy, která nemá dostatečné finanční prostředky na plnohodnotné komerční produkty. Druhotným cílem práce bude porovnávání komerčních produktů s open source produkty a hledání různých nahraditelných kombinací.

Vytvořená vzorová konfigurace bude v praktické části práce porovnána s konfigurací vybrané firmy a budou analyzovány odlišnosti. Jinými slovy lze tedy říci, že ve vybrané firmě bude proveden bezpečnostní audit.

Na základě výsledků budou vyzdvihnuty silné stránky vybrané lokální sítě, ale hlavním cílem tohoto bezpečnostního auditu bude naopak nalezení slabých míst, které mohou představovat potenciální riziko pro ohrožení bezpečnosti. Pro každé slabé místo bude na základě optimální konfigurace navrženo doporučení, které by mělo dané riziko omezit nebo nejlépe úplně odstranit. Součástí těchto doporučení bude i jejich finanční nákladnost, která bude posléze zvážena s přihlédnutím k rozpočtu vybrané firmy. Konečným výsledkem by tedy měl být seznam určitých doporučení, které budou pro vybranou firmu realizovatelné v rámci rozpočtu.

3 Literární rešerše

3.1 Teoretické základy lokální sítě – OSI model

Local Area Network (též LAN, lokální síť, místní síť) označuje v informatice malou síť, která umožňuje komunikaci mezi propojenými počítači. Jedná se o sítě uvnitř místností, budov nebo malých areálů; ve firmách i v domácnostech. Slouží ke snadnému sdílení prostředků, které jsou v lokální síti dostupné. Lokální síť umožňuje sdílení diskového prostoru, internetu, intranetu, tiskáren, IS atd.

Model ISO/OSI je komunikační model označený zkratkou slovního spojení "International Standards Organization / Open Systen Interconnection" (Mezinárodní organizace pro normalizaci / propojení otevřených systémů). Model byl definovaný organizací ISO v roce 1983 a rozděluje komunikaci mezi 2 počítači do sedmi vrstev, které jsou též známé jako Sada vrstev protokolu.

Úkolem každé vrstvy je poskytovat služby následující vyšší vrstvě a nezatěžovat vyšší vrstvu detaily o tom, jak je služba ve skutečnosti realizována. Pro jakýkoliv přesun dat mezi vrstvami jsou data rozdělena na packety. V každé vrstvě se pak k paketu přidávají další doplňkové informace (formátování, adresa), které jsou nezbytné pro úspěšný přenos po síti.

Popis OSI modelu vznikl již před řadou let a přesto, že se považuje za základ pro síťové technologie, tak nebyl nikdy přesně realizován. Obdobou OSI modelu je TCP/IP, u kterého můžeme říci, že vychází z OSI modelu, ale upravuje jej, aby byl více flexibilní. Podle OSI modelu je vždy možno komunikovat pouze s vrstvou nad nebo pod. A všechny vrstvy musí být v komunikaci obsaženy, což v řadě praktických úloh přináší zbytečnou zátěž (časovou i datovou). Přesto je OSI model dobrý pro výklad a teoretický popis vývoje a struktury sítí. [1]

[1] *OSI Model – SAMURAJ-cz.com* [online]. c2007, poslední revize 05.03.2007 [cit. 2010-02-03]. Dostupné z <http://www.samuraj-cz.com/clanek/osi-model/>.

Anglický název	Český název	Jednotka	Funkce vrstvy	Využití v praxi
Application	Aplikační	Data	Síťové procesy pro aplikaci, ověření uživatelů, vše závislé na aplikaci.	Telnet, FTP
Presentation	Prezentační	Data	Reprezentace dat a šifrování. Řeší rozdíly v reprezentaci dat mezi aplikací a síťovým formátem - kóduje data pro přenos.	MIDI, MPEG
Session	Relační	Data	Spojení mezi aplikacemi, správa session. Komunikace jedné aplikace s druhou, posílání více dat po sobě. Udržuje celé spojení mezi dvěma počítači.	NetBIOS
Transport	Transportní	Segments (segmenty)	End-to-end spojení systémů, spolehlivost - zajišťuje kompletní přenos dat, kvalita služby. Řeší spolehlivé odeslání všech dat ze zdroje do cíle pomocí segmentace a potvrzování.	TCP, UDP
Network	Síťová	Packets (pakety)	Logická adresace - routování - určení cesty paketu, přenos dat z bodu do bodu, používá IP adresy. Komunikace mezi zdrojovým a cílovým zařízením pomocí IP adresy.	IP, ICMP, ARP, RIP
Data Link	Linková	Frames (rámce)	Fyzická adresace, MAC - media access control a LLC - logical link control, datový tok, synchronizace rámů, komunikace 1 hop, používá MAC adresy. Detekce chyb, řízení toku a přístupu na médium. Komunikace mezi dvěma zařízeními v jednom subnetu (nebo na bránu) pomocí MAC adresy. Vytváří rámce (hlavička + data + zápatí).	Ethernet, FDDI, Token Ring, PPP, SLIP
Physical	Fyzická	Bits (bity)	Fyzické parametry linky - média (kabely, rádio, světlo), signály a binární přenos. Řeší fyzické poslání dat (přenášeným bitům nepřiřazuje žádný význam).	100BaseT, RS-232, 802.11

Tabulka 1 – OSI model, zdroj: http://www.samuraj-cz.com/clanek/osi-model/

Hlavní odlišnosti mezi referenčním modelem ISO/OSI a TCP/IP vyplývají především z rozdílných výchozích předpokladů a postojů jejich tvůrců. Při koncipování

referenčního modelu ISO/OSI měli hlavní slovo zástupci spojových organizací. Ti pak nově vznikajícímu modelu vtiskli svou vlastní představu - především spojovaný a spolehlivý charakter služeb, poskytovaných v komunikační podsíti (tj. až do úrovně síťové vrstvy, včetně). Jinými slovy: ISO/OSI model počítá se soustředěním co možná nejvíce funkcí, včetně zajištění spolehlivosti přenosů, již do komunikační podsítě, která v důsledku toho bude muset být poměrně složitá, zatímco k ní připojované hostitelské počítače budou mít relativně jednoduchou úlohu. Později se ale ukázalo, že například právě v otázce zajištění spolehlivosti to není nejšťastnější řešení - že totiž vyšší vrstvy nemohou považovat spolehlivou komunikační podsíť za dostatečně spolehlivou pro své potřeby, a tak se snaží zajistit si požadovanou míru spolehlivosti vlastními silami. V důsledku toho se pak zajišťováním spolehlivosti do určité míry zabývá vlastně každá vrstva referenčního modelu ISO/OSI.

Tvůrci protokolů TCP/IP naopak vycházeli z předpokladu, že zajištění spolehlivosti je problémem koncových účastníků komunikace, a mělo by tedy být řešeno až na úrovni transportní vrstvy. Komunikační podsíť pak podle této představy nemusí ztrácet část své přenosové kapacity na zajišťování spolehlivosti (na potvrzování, opětné vysílání poškozených paketů atd.), a může ji naopak plně využít pro vlastní datový přenos. Komunikační podsíť tedy podle této představy nemusí být zcela spolehlivá - může v ní docházet ke ztrátám přenášených paketů, a to bez varování a bez snahy o nápravu. Komunikační síť by ovšem neměla zahazovat pakety bezdůvodně. Měla by naopak vyvíjet maximální snahu přenášené pakety doručit (v angličtině se v této souvislosti používá termín: best effort), a zahazovat pakety až tehdy, když je skutečně nemůže doručit - tedy např. když dojde k jejich poškození při přenosu, když pro ně není dostatek vyrovnávací paměti pro dočasné uložení, v případě výpadku spojení apod. Na rozdíl od referenčního modelu ISO/OSI tedy TCP/IP předpokládá jednoduchou (ale rychlou) komunikační podsíť, ke které se připojují inteligentní hostitelské počítače.[2]

Praktický rozdíl mezi OSI modelem a TCP/IP je ukázán v následující tabulce, kde můžeme vidět, že u TCP/IP došlo skutečně k optimalizaci a tedy snížení časové i datové náročnosti.

[2] *Síťový model TCP/IP* [online]. c2006 [cit. 2010-02-03]. Dostupné z <http://pc-site.owebu.cz/?page=PTCPIP>.

TCP/IP	OSI
	Aplikační
	Prezentační
Aplikační	Relační
Transportní	Transportní
Síťová	Síťová
	Linková
Vrstva síťového rozhranní	Fyzická

Tabulka 2 – OSI a TCP/IP porovnání

3.1.1 TCP/IP

Transmission Control Protocol/Internet Protocol (česky primární transportní protokol - TCP/protokol síťové vrstvy - IP) je v současnosti hlavním protokolem celosvětové sítě Internet. Komunikační protokol je množina pravidel, které určují syntaxi a význam jednotlivých zpráv při komunikaci. Komunikace mezi stejnými vrstvami dvou různých systémů je řízena komunikačním protokolem za použití spojení vytvořeného sousední nižší vrstvou. Architektura umožňuje výměnu protokolů jedné vrstvy bez dopadu na ostatní. Příkladem může být možnost komunikace po různých fyzických médiích - ethernet, optické vlákno, sériová linka.

Architektura TCP/IP je členěna do čtyř vrstev na rozdíl od referenčního modelu OSI se sedmi vrstvami, jak je ukázáno v tabulce 2.

1) Vrstva síťového rozhraní

Nejnižší vrstva umožňuje přístup k fyzickému přenosovému médiu. Je specifická pro každou síť v závislosti na její implementaci. Příklady sítí: Ethernet, Token ring, FDDI, X.25, SMDS.

2) Síťová vrstva

Vrstva zajišťuje především síťovou adresaci, směrování a předávání datagramů. Protokoly: IP, ARP, RARP, ICMP, IGMP, IGRP, IPSEC. Je implementována ve všech prvcích sítě - směrovačích i koncových zařízení.

3) Transportní vrstva

Transportní vrstva je implementována až v koncových zařízeních (počítačích) a umožňuje proto přizpůsobit chování sítě potřebám aplikace. Poskytuje spojované (protokol TCP, spolehlivý) či nespojované (UDP, nespolehlivý) transportní služby.

4) Aplikační vrstva

Vrstva aplikací. To jsou programy (procesy), které využívají přenosu dat po síti ke konkrétním službám pro uživatele. Příklady: Telnet, FTP, HTTP, DHCP, DNS.

Aplikační protokoly používají vždy jednu ze dvou základních služeb transportní vrstvy: TCP nebo UDP, případně obě dvě (např. DNS). Pro rozlišení aplikačních protokolů se používají tzv. porty, což jsou domluvená číselná označení aplikací. Každé síťové spojení aplikace je jednoznačně určeno číslem portu a transportním protokolem (a samozřejmě adresou počítače).[3]

3.2 Zabezpečení na hardwarové úrovni

V této kapitole budou probrány možnosti pro zabezpečení lokální sítě na hardwarové (fyzické) úrovni.

3.2.1 Infrastruktura

Infrastruktura je základní kámen pro provozování jakékoliv počítačové sítě. Cílem každé infrastruktury je promyšlené rozvržení všech počítačových (a eventuelně komunikačních) prvků. Každý uživatel by měl mít dostupné potřebné prostředky, aby mohl vykonávat svou práci. Cílem infrastruktury je také vytvoření minimální pasivní ochrany síťových prvků, aby byl omezen přístup neznámým uživatelům k citlivým datům či službám. Důležité síťové prvky (jako např. souborový/poštovní server a další typy serverů, záložní komponenty, Wi-Fi přístupové body atd.) by měly být umístěny tak aby se k nim nemohl dostat nezvaný návštěvník nebo nešikovný pracovník. Optimální umístění je v malé klimatizované místnosti, kterou je možné uzamykat. Klimatizované místnosti poskytují sníženou vlhkost vzduchu a stabilní teplotu, což jsou

[3] *TCP/IP – Wikipedie, otevřená encyklopedie* [online]. c2007, poslední revize 5.02.2009 [cit. 2010-02-21]. Dostupné z < http://cs.wikipedia.org/wiki/TCP/IP >.

faktory, které mají vliv na životnost daných komponent. V takovýchto podmínkách není možné dlouhodobě pracovat, a proto je vhodné, aby veškerá možná správa byla prováděna přes vzdálenou kontrolu.

Co týče kabelových rozvodů a Wi-Fi přístupových bodů, tak jejich rozvržení by mělo odpovídat potřebám firmy a její velikosti. Je samozřejmě vhodné, když jsou přípojkové kapacity lehce předimenzovány, aby nemuselo docházet ke složitým rekonstrukcím při postupné expanzi firmy. Zároveň je vhodné, aby veškeré přístupové body byly zabezpečeny proti přístupu nezvaných návštěvníků. Samotné zabezpečení přístupových bodů je většinou prováděno na softwarové úrovni což bude probráno v kapitole 3.3 a 3.4.

3.2.2 Síťové prvky s integrovanou ochranou

Mnoho současných síťových prvků nabízí možnost zabezpečení prostřednictvím integrovaných firewallů a dalších bezpečnostních řešení. Tyto prvky fungují na stejném principu jako např. softwarový firewall, ale odpadá nutnost instalace daného firewallu atd. Pro malé firmy, které nemají dostatečné finanční dispozice, může být dobrou alternativou pořídit router s integrovaným firewallem než nákladně zřizovat server. Nabídkové spektrum je velice pestré a lze pořídit levné modely do 5.000Kč. Pro potřeby malé až střední firmy je výhodnou koupí např.: Cyberoam CR15i. Tento router se prodává za 11.901Kč (průměrná hodnota z 3 náhodných e-shopů z 25. 2. 2010) a nabízí následující služby:

- Statefull Inspection Firewall s ICSA Labs certifikací
- VPN brána
- Anti-spyware, anti-virus, anti-spam
- IPS
- URL a aplikační filtrace
- Řízení šířky pásma, QoS
- Definice politik na základě identity uživatele
- Doporučené využití pro max. 15 uživatelů
- VPN

Na základě výše uvedených specifikací lze konstatovat, že produkt Cyberoam CR15i je výborné komplexní řešení k zabezpečení téměř jakékoliv malé sítě či segmentu větší sítě. Tento router v sobě obsahuje v podstatě veškeré potřebné služby, které jsou potřeba k zabezpečení a správě sítě. Z ekonomického hlediska se jedná o výhodnou investici pro jakoukoliv firmu, která by ráda centralizovala svoje zabezpečení či plánuje budovat novou lokální síť.

S ohledem na výše uvedená pozitiva je nutné uvést, že pro ještě lepší zabezpečení je vhodné kombinovat hardwarový a softwarový firewall a další programy jako např. antivirový atd.

Levnější alternativa pro výše uvedený Cyberoam CR15i lze uvést ZyXEL P-792H jehož specifikace jsou následující:

- Firewall
- Plnohodnotná kontrola paketů
- Prevence Prevent DoS a DDoS útoků
- Kontrola přístupů dle práv
- Filtrování obsahu
- Filtrování paketů
- Logování a výstrahy útoků v reálném čase
- Virtuální privátní síť (VPN)
- DES, 3DES a AES šifrování
- VPN

V porovnání s produktem Cyberoam CR15i je funkční spektrum výrazně chudší, jelikož chybí služby jako IPS, anti-spyware, anti-spam a další. Cena routeru ZyXEL P-792H je 4.951Kč (průměrná hodnota z 3 náhodných e-shopů z 25. 2. 2010). Cenově se teda jedná o poloviční cenu oproti Cyberoam CR15i. Pokud bychom ZyXEL P-792H brali pouze jako doplňkový bezpečnostní prvek, tak by se jednalo o výhodnou koupi, ale pokud firma hledá plnohodnotný router, který nabídne komplexní zabezpečení a správu lokální sítě, tak je Cyberoam CR15i jednoznačně výhodnější varianta.

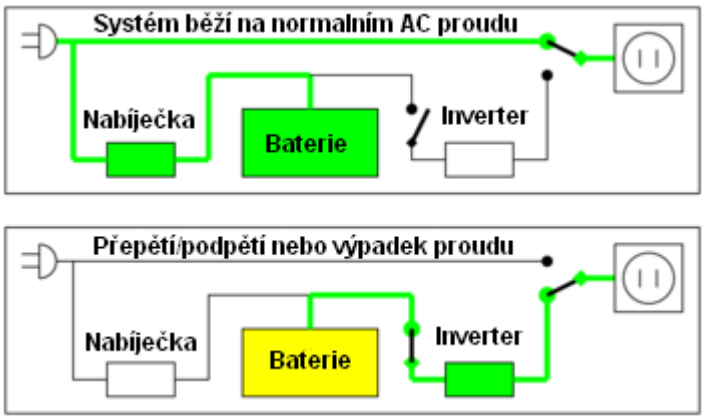
Jak bylo ukázáno na 2 porovnaných produktech tak s úměrně s cenou klesá funkční nabídka. Routery s cenou pod 5.000Kč lze vhodně využívat jako doplňkové prvky v zabezpečení lokální sítě a pro plnohodnotné komplexní řešení jsou vhodné

produkty s cenou od 10.000Kč. Pokud firma nedisponuje velkými finančními prostředky tak lze brát např. ZyXEL P-792H jako dostatečné řešení, ale pro plnohodnotnou ochranu je určitě vhodné investovat do dražších modelů.

3.2.3 UPS

UPS (z anglického Uninterruptible Power Supply) je zařízení, které dodává elektřinu pro zařízení či komponenty, které nesmějí být neočekávaně vypnuty. Důvodem vypnutí může být výpadek, nárazové přepětí či podpětí nebo celkově nestabilní dodávka elektrické energie.

UPS je tzv. nepřerušitelný zdroj energie, který je ve většině případů zapojen jako mezičlánek mezi zdroj elektřiny a vstup napětí daného zařízení. UPS obsahuje akumulátory, které jsou udržovány v nabitém stavu, aby UPS mohlo kdykoliv poskytnout záložní zdroj energie. V okamžiku přerušení dodávky elektřiny zajišťuje UPS napájení zařízení až do svého vybití, obnovení dodávky nebo do momentu kdy jsou zařízení automaticky vypnuta.



Obrázek 1 - Princip UPS

Kapacita akumulátorů má největší vliv na výdrž UPS, která se pohybuje od několika minut po několik hodin. Akumulátory jsou vyráběny různými technologiemi a může u nich docházet ke kolísání kvality v případě zvolení levného řešení. I renomovaní výrobci poskytují v dnešní době záruční lhůtu na akumulátory na pouhých 12 měsíců, což svědčí o značném vlivu stáří na celkovou výdrž.

UPS je schopné eliminovat následující hrozby:

- ztráta napájení
- krátkodobý pokles (Velmi krátkodobý pokles napětí o 15-20%)
- napěťová špička (Krátkodobé přepětí o více než 10% -může způsobit poškození zařízení)
- změna frekvence
- dlouhodobé podpětí či přepětí
- elektromagnetické rušení
- napěťové rázy (mžikové špičky až 20 000V, způsobovány přeskokem jisker při spínání a elektrostatickými výboji)
- harmonické zkreslení

Zcela zásadní využití UPS je jako zdroj záložní energie pro klíčové síťové prvky, kterými jsou servery, zálohovací prvky atd. Jakýkoliv výpadek může způsobit nedostupnost potřebných služeb nebo poruchu hardwarových komponent. Některé hardwarové komponenty (např. RAM, harddisk, procesor) jsou citlivé na kvalitní dodávku elektrické energie. Velké množství elektrických rozvodů je v dnešní době zastaralé a dodávaný el. proud obsahuje různé ruchy a výkyvy.

I přes to, že UPS je schopné dodávat náhradní energii pouze po dobu několika desítek minut, tak je to ve většině případů dostatečné, protože pouze výjimečně dochází k výpadkům delším než cca 15 minut. Využití UPS pro jednotlivé firemní počítače je závislé na pracovní náplni dané firmy a finančních prostředcích. Naopak využití UPS pro jakékoliv serverové komponenty je zcela klíčové a mělo by být standardem v každé firmě bez ohledu na velikost.

3.2.3.1 Komerční řešení UPS

Dlouholetým standardem v kategorii UPS je firma APC, která nabízí produkty jak pro domácnost, tak pro firmy, které mají nejvyšší požadavky. Nejlevnější řešení, které ja v nabídce firmy APC je model APC Back-UPS CS 350. Průměrná cena tohoto modelu je 2.237Kč (průměrná hodnota byla spočítána na základě cen z 3 náhodně vybraných obchodů kde dni 19. 2. 2010). Model APC Back-UPS RS 800 je zařazen

zhruba uprostřed nabídkového spektra a představuje optimální výbavu a výkon za cenu 4.457Kč (průměrná hodnota byla spočítána na základě cen z 3 náhodně vybraných obchodů kde dni 19. 2. 2010). Tento model je vybaven bezúdržbovými bateriemi, komunikačním rozhraním USB a 6 výstupními zásuvkami. Prostřednictvím komunikačního rozhraní lze řídit baterie, monitorovat stav el. sítě či konfigurovat UPS pro různé krizové stavy.

Model RS 800 je vhodným řešením pro malé až střední firmy. V podstatě lze konstatovat, že i model CS 350 splní svojí funkci dobře, ale bude schopen dodávat energii pouze v řádu několika minut. Pokud by během výpadku začaly servery automaticky ukládat data, postupně se vypínat a došlo by k vyčerpání záložní energie, tak by mohly být způsobeny ještě větší škody než bez UPS. Je určitě vhodnější pořídit alespoň minimálně předimenzované UPS, které poskytne dostatečnou rezervu pro všechny předpokládané scénáře.

3.2.4 IEEE 802.1X

IEEE 802.1X je protokol, který lze použít pro zabezpečení fyzického přístupu do počítačové sítě. Sebelepší infrastruktura může mít slabá místa, které umožní potenciálnímu útočníkovi, aby se připojil do lokální sítě. Pokud je do síťového portu připojeno zařízení, tak je daný port zablokován, dokud nedojde k autentizaci připojeného zařízení. Jediný povolený typ komunikace je povolen přes port EAP, který zajišťuje autentizaci.

Samotný protokol 802.1X zabezpečuje pouze samotný vstup do lokální sítě a jakmile se útočníkovi podaří dostat skrz tuto ochranu, tak může libovolně využívat služby dané lokální sítě. Jedná se tedy pouze o jednu z mnoha dalších úrovní zabezpečení.

Protokol 802.1X lze provozovat na všech operačních systémech Windows počínaje verzi 2000. Protokol podporuje i Linux a MacOS a jedná se tedy multi-platformové řešení, které je vhodné k částečnému (jak již bylo zmíněno tak se jedná pouze o další stupeň ochrany) zabezpečení vstupu do lokální sítě.

3.3 Zabezpečení na softwarové úrovni

Bezpečnost Intranetu/LAN je silně závislá na operačních systémech, programech (nainstalovaných na firemních počítačích) a v hlavní míře na správném nastavení všech aspektů, které budou probrány v dalších kapitolách.

3.3.1 Operační systémy a uživatelské skupiny

V této kapitole nebudou dlouze porovnávány druhy operačních systémů. Podrobný rozbor by stačil na samostatnou bakalářskou/diplomovou práci. Drtivý většinový podíl na domácím i firemním trhu zabírají operační systémy firmy Microsoft. Tyto operační systémy jsou dobře známy pro svoje klady i zápory. Na druhé straně jsou zde Open source operační systémy založené na jádře Linux. Jejich nespornou výhodou je mnohem vyšší úroveň zabezpečení celého systému a zároveň rychlejší provoz na stejné sestavě. Nevýhodou je celkově složitější systém, který vyžaduje pokročilejšího uživatele a eventuelně bude zapotřebí dodatečné školení pro neznalé zaměstnance. Další nevýhodou téměř všech operačních systémů založených na jádře Linux je jejich kompatibilita s různými komponenty. Vzhledem k povaze Open source je logické, že není v silách všech dobrovolných programátorů vytvářet ovladače pro každou revizi všech možných komponent. Toto bohužel vede k dosti nepříjemným problémům s instalací takovýchto operačních systémů. Pokud se podaří úspěšně nainstalovat a nakonfigurovat tento druh systému, tak se jedná o mnohem bezpečnější a leckdy i stabilnější operační systém než produkty firmy Microsoft.

Operační systémy na bázi Linuxu mají mnoho mutací, ať už se jedná o volně stažitelné verze či normální komerční produkty a mnohdy je problém vybrat vhodné řešení pro uživatelovy znalosti a potřeby. Operační systémy firmy Microsoft se na trhu vyskytují pouze jako 3 produkty (různé typy jako Home, Professional či Ultimate budou v této práci ignorovány, jelikož pro kancelářské využití se hodí pouze Professional či Ultimate a liší se pouze výbavou). V současnosti je nejpoužívanější operační systém Windows XP, který dosáhl již třetího opravného balíčku (Service Pack 3) a dal by se považovat za odladěný systém. Nástupcem Windows XP byl Windows Vista, který byl považován za propadák vzhledem k velkým a zbytečným hardwarovým nárokům a jiným důležitým nedostatkům. Opravdovým nástupcem verze XP jsou Windows 7,

které spojily výhody systémů XP a 7. Poskytují rychlé a uživatelsky přívětivé GUI a jejich hlavní devizou je stabilita. Budoucnost ukáže, jak Windows 7 ustojí útoky různých hackerů a zdali bude také potřeba tolik opravných balíčků.

Lze tedy konstatovat, že pokud má uživatel pokročilé znalosti s používáním počítačů, tak je pro něj vhodné používat operační systém na jádře Linux. V současné době je vzájemná kompatilibita mezi Open source s Microsoft operačními systémy téměř bezproblémová. Není tedy problém provozovat např. 3 počítače s Open source operačním systémem a 10 počítačů s operačním systémem Windows 7.

3.3.1.1 Vytváření a správa uživatelských skupin a práv

Všechny operační systémy vyjmenované v předchozí kapitole umožňují spravovat uživatelské účty na téměř identickém principu. V jakékoliv firmě by bez ohledu na její velikost měla být zřízena určitá pracovní a tedy i uživatelská hierarchie. Uživatelé jsou rozděleni prostřednictvím skupin, které mají definovány odlišná práva. Tyto práva se týkají omezení působnosti uživatelů dané skupiny a opravňují/povolují uživatelům používat různé funkce nebo pracovat s určitými soubory.

Standardní nastavení uživatelských účtů je možné upravit a zvýšit bezpečnost operačního systému. Při této činnosti si musíme uvědomit, že každé zvýšení bezpečnosti zároveň snižuje funkčnost systému (vždy provedeme restrikci, která omezí nějakou funkci). Proto je dobré každý krok pečlivě promyslet a jednotlivé restrikce provádět postupně. Po zavedení omezení je vždy vhodné vyzkoušet funkčnost sytému a teprve poté provést další restrikci.[4]

Je vhodnější, aby se administrátor řídil podle pesimistického scénáře a automaticky předpokládal, že uživatel bude mít práva pouze k vykonávání pracovní náplně a pokud bude vyžadovat něco nadstandardně tak bude muset požádat o dodatečné povolení. Toto může vést k množícím se žádostem, ale pokud je celý systém nastaven rozumně a s „citem“, tak by každý zaměstnanec měl dostatečná práva a neměl by být omezován ve vykonávání své práce. Tato přísná bezpečnostní politika je vhodná do středních až větších firem nebo do malých firem, kde je vyžadována nadstandardní

[4] HORÁK, Jaroslav. Bezpečnost malých počítačových sítí. 1. vydání. Praha: Grada, 2003. 200 s. ISBN 80-247-0663-6. Kapitola 1.3, Zesílení ochrany uživatelských účtů, s. 25

bezpečnost. Pokud se jedná o malou firmu, kde se zaměstnanci mezi sebou znají, tak je možné zavést volnější uživatelská práva.

U správy uživatelů by mělo být samozřejmostí deaktivovat funkce jako Auto-logon či účet Guest.

3.3.1.2 Active Directory a domény

Active Directory umožňuje administrátorům nastavovat politiku, instalovat programy na mnoho počítačů nebo aplikovat kritické aktualizace v celé organizační struktuře. Active Directory ukládá své informace a nastavení v centrální organizované databázi.
Adresářová služba Active Directory je rozšiřitelná a škálovatelná adresářová služba, která umožňuje efektivně uspořádat síťové prostředky.

- *vyžaduje instalaci služby DNS*
- *je založena na standardních internetových protokolech*
- *jednoznačně definuje strukturu sítě*
- *organizuje skupiny počítačů a domén*[5]

Doména je základním prvkem v logické architektuře Active Directory. Doména sestává z objektů, což jsou např. servery, aplikace, uživatelé atd. Doména nemusí být provozována pouze na lokální síti, ale může se rozprostírat jakkoliv – není omezena na fyzickou lokaci. Hlavní výhodou domény oproti běžné uživatelské skupině je možnost zabezpečení a konfigurace. Jedním z mnoha příkladů zabezpečení je např. omezení špatných loginů čímž se dá eliminovat možnost prolomení hesla.

Domény a Active Directory mají své využití ve středních a velkých firmách, kde je možnost vytvářet velmi komplexní architektury. Toto řešení lze samozřejmě aplikovat i na menší firmy, které buď mají nezvyklou architekturu (např. více poboček) nebo prostě vyžadují lepší systém zabezpečení uživatelských účtů a celé lokální sítě.

[5] *Active Directory – Wikipedie, otevřená encyklopedie* [online]. c2005, poslední revize 16.09.2009 [cit. 2010-02-20]. Dostupné z <http://cs.wikipedia.org/wiki/Active_Directory>.

3.3.2 Vytváření a administrace hesel

Základním prvkem všech bezpečnostních opatření je heslo. Heslo může splňovat úlohu autentizace spolu s přihlašovacím jménem, které slouží k identifikaci daného uživatele. Heslo může být také použito samostatně bez jakýchkoliv jiných údajů. Je nutné vycházet z předpokladu, že jakékoliv heslo je prolomitelné a nejdůležitějším faktorem v tomto případě je čas. Doba nutná k prolomení hesla se v dnešní době zkracuje vzhledem k neustále vzrůstajícímu výpočetnímu výkonu. K prolomení hesla se používají různé metody, ale nejznámější a nejpoužívanější je bezesporu tzv. Brute force útok. Tato metoda systematicky testuje všechny možné kombinace, dokud není heslo nalezeno. Rychlost této metody je přímo závislá na výpočetním výkonu daného počítače. Za účelem zvýšení výkonu začaly být používány v současnosti i grafické karty k takovýmto výpočtům.

Silné heslo je obtížně prolomitelné což je dáno následujícími podmínkami:

1) V důsledku principu šifrování jsou nejbezpečnější hesla obsahující 7 nebo 14 znaků tzn. délka nejméně 7 znaků

*2) Obsahuje znaky ze všech tří následujících skupin: písmena (velká a malá), číslice a symboly (např. @ # $ * ^)*

3) Obsahuje nejméně jeden symbol, umístěný na druhé až šesté pozici

4) Pokud dochází k pravidelným změnám u hesla, je nutné, aby se nové heslo výrazně lišilo od starého

5) Neobsahuje uživatelské jméno, ani jméno/příjmení uživatele účtu

6) Nejedná se o běžné slovo či jméno[6]

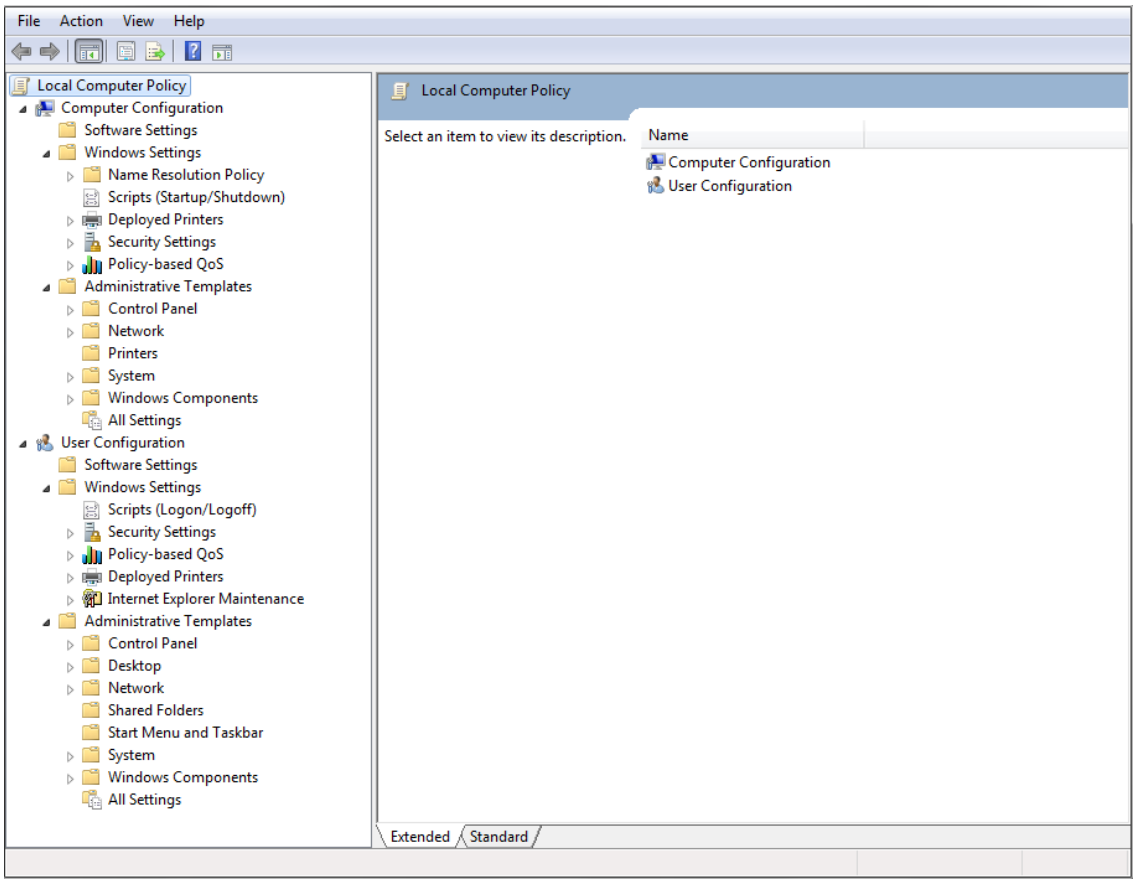
Je zřejmé, že ne každý uživatelský účet vyžaduje silné heslo. Ve všech případech by i základní hesla měla splňovat podmínky 1, 5 a 6.

Pokud bezpečnostní politika vyžaduje výměnu hesel na pravidelné bázi tak je doporučeno provádět tyto operace každých 60 až 90 dní v závislosti na přísnosti dané politiky.

[6] HORÁK, Jaroslav. Bezpečnost malých počítačových sítí. 1. vydání. Praha: Grada, 2003. 200 s. ISBN 80-247-0663-6. Kapitola 1.3, Zesílení ochrany uživatelských účtů, s. 26

3.3.3 Správa uživatelských účtů prostřednictvím konzole MMC Zásady skupiny

Ve Windows XP a dále je možné vytvořit základní zásady, které budou platit pro všechny uživatele, což může dosti zásadně ovlivnit zabezpečení operačních systémů a celé lokální sítě. Spuštění konzole Zásady skupin je provedeno příkazem GPEDIT.MSC (Start – Spustit).



Obrázek 2 – Konzole MMC Zásady skupin

Vzhled konzole MMC je ukázán na obrázku 2. Jak lze vidět, tak je možné aplikovat jakékoliv nastavení buď pro uživatele, nebo celý počítač.

Prostřednictvím tohoto nástroje je možné globálně upravovat nastavení pro bezpečnostní kategorie jako např.:

- Hesla – Maximální a minimální stáří hesla, minimální délka hesla, vynucení používání historie hesel, požadavky na složitost hesla
- Uzamykání účtů – Prahová hodnota pro zamčení účtu, doba uzamknutí účtu atd.

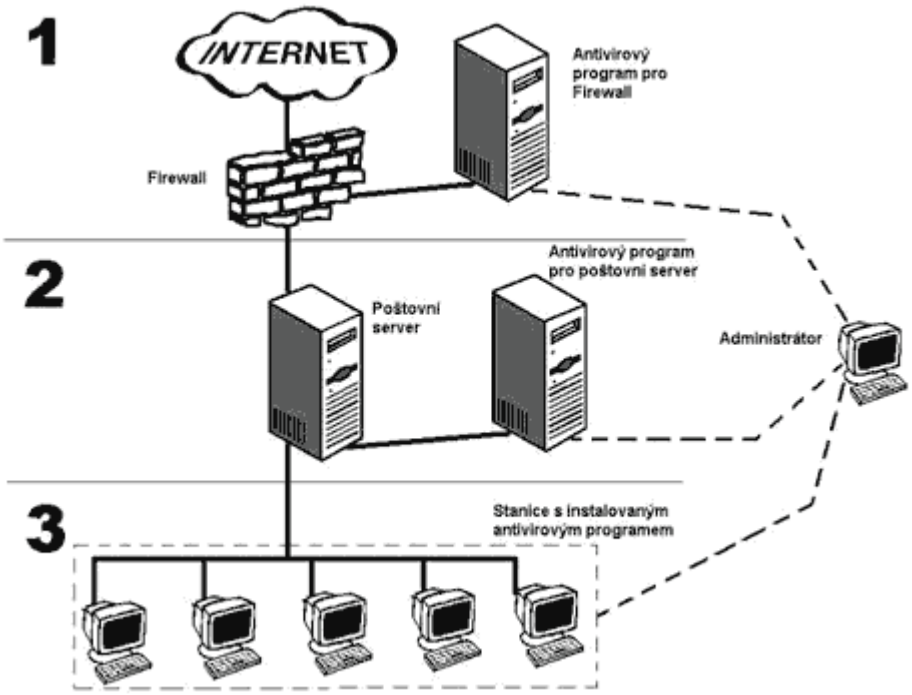
Mimo jiné lze konfigurovat i jiné faktory, které se týkají chodu operačního systému a uživatelů. Jedná se výborný nástroj pro jednoduchou a zároveň velmi efektní správu uživatelských účtů.

3.3.4 Antivirové programy

Důležitost antivirových programů je v dnešní době nepopíratelná a jejich přítomnost na počítači se stala více méně standardem. Pro běžného pracovníka nehraje roli, jakým způsobem byl infikován (zdali útočník byl klasický počítačový virus, e-mailový červ, trojský kůň nebo jakýkoliv jiný druh škodlivého kódu), ale že jakákoliv infekce může ohrozit integritu firemních dat, bezpečnost celé lokální sítě a tedy přímo ovlivnit konkurenceschopnost dané firmy. Přítomnost antivirového programu v jakékoliv firemní síti je nezbytná.

Současným trendem v oblasti antivirových programů je vytváření víceúrovňové antivirové ochrany. Tato ochrana by měla sestávat minimálně ze dvou a v optimálním případě ze tří úrovní (v závislosti na infrastruktuře dané lokální sítě). Za základní úroveň je považován antivirový program na pracovní stanici, další úroveň může být ochrana poštovního či souborového serveru a poslední úroveň ochrany by měl být antivirový program na internetové vstupní bráně. Celý systém víceúrovňové ochrany je zobrazen na obrázku 3. V takovémto řešení je zároveň klíčové aby administrátor mohl spravovat různé úrovně ochrany z jednoho počítače či ze vzdáleného počítače, který bude mimo danou lokální síť a zároveň pod vlastní úrovní ochrany.

Pokud jsou tedy na pracovních stanicích instalované antivirové programy, tak je velmi důležité aby samotní uživatelé nebyli obtěžováni zprávami antivirového programu a aby neměli možnost jakkoliv pozměnit nastavení.



Obrázek 3 – Víceúrovňová architektura, zdroj: http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=188&clanekID=196

Hlavní výhody víceúrovňové architektury jsou následující:

- V případě selhání (ať už jde o nechtěný výpadek či prolomení bezpečnosti) jakékoliv úrovně je stále minimálně jedna úroveň v provozu
- Celá lokální síť je chráněna i proti internímu útoku, který může přijít např. od neopatrného zaměstnance, který otevře infikovanou přílohu či stáhne do počítače infikovaný soubor z přenosného média

Antivirové programy jsou nabízeny v nespočetném množství verzi a od mnoha výrobců. Mezi nejznámější výrobce patří např.: ESET, AVG, Norton, McAfee, F-Secure. Rozdíly mezi danými řešeními jsou měřitelné, ale ve většině případů se jedná o rozdílnost ve výkonnosti, přičemž nejdůležitějším faktorem je vždy schopnost odhalovat škodlivý kód. Velkou výhodou může být např. přítomnost více vyhledávacích antivirových motorů, které zásadně zlepšují účinnost odhalovaní škodlivého kódu.

Za zmínku stojí i pokročilé řešení, které kombinuje speciální hardware a software a ve společné kombinaci se jedná o účinný a rychlý nástroj. Důvodem proč není toto řešení detailně analyzováno, je poměrně vysoká pořizovací cena.

3.3.5 Firewall

Firewall je zařízení, které prostřednictvím různých pravidel řídí a zabezpečuje síťový provoz mezi sítěmi s odlišnou úrovní důvěryhodnosti a zabezpečení. Firewall představuje první linii zabezpečení lokální sítě před útočníky z venkovní sítě (nejčastěji internet). Druhou obrannou linií bývá nejčastěji IDS či IPS systém, který detekuje či filtruje potenciální útoky, které nebyly zachyceny firewallem. V praxi mohou tedy nastat 4 situace:

1) Nežádoucí provoz je správně detekován jako útok
2) Nežádoucí provoz není detekován a útok je úspěšný
3) Řádný provoz je nesprávně označen jako útok
4) Řádný provoz je ověřen jako dobrý

Je logické, že žádoucí situace jsou pouze 1. a 4. Situace 2. a 3. jsou nežádoucí a jejich výskyt by měl být minimalizován.

Problémem současných firewallů je jejich vysoká cena. Vzhledem k celkové důležitosti firewallu je opravdu nutné si za kvalitu připlácet, což pro většinu malých firem není vhodné.

Příkladem komerčního firewallu je produkt Kerio WinRoute Firewall od firmy Kerio. Tento produkt je nabízen ve třech variantách, které jsou porovnány v následující tabulce. Pro účely porovnání byl do tabulky zahrnut i router Cyberoam CR15i (viz kapitola 3.2.2), který nabízí podobné služby.

Produkt	**Cena (pro 15 uživatelů)**
Kerio WinRoute Firewall s McAfee Anti-virus	11.385Kč
Kerio WinRoute Firewall	9.488Kč
Kerio Web Filter	3.832Kč
Cyberoam CR15i	11.901Kč

Tabulka 3 - Cenové porovnání firewallů

Jak lze vidět v tabulce 3, tak cena firewallu (včetně antivirového programu) pro 15 uživatelů je zhruba stejná jako cena routeru, který nabízí minimálně srovnatelné funkce. Detailní porovnání funkcí bude probráno v kapitole 4.1.

Stejně jako u antivirových programů tak i u firewallů je vhodné využívat více úrovní v zabezpečení. Optimální řešení je např. umístění prvního firewallu na vstupní bránu do lokální sítě a zároveň provozovat firewall na jednotlivých pracovních stanicích. Na daných pracovních stanicích je možné prostřednictvím firewallu řídit jednotlivé procesy.

Vzhledem k tomu, že spousta dnešních firewallů funguje v prostředí operačních systémů Linux, tak je možné vytvořit více úrovňovou multi-platformovou firewall architekturu. V praxi se málokdy stává, aby útočník měl dostatečné zkušenosti a prostředky aby se mu podařilo prolomit Linux firewall a následně Windows firewall. Pokud je daný útočník specialista např. na Linux firewall, tak po prolomení dané Linux firewall se musí přeorientovat na jiný druh firewall což zabírá čas. Čas je v tomto případě zcela klíčovým faktorem, protože čím déle trvá útočníkovi prolomení prvků ochrany, tím je větší šance, že bude jeho útok odhalen a potlačen.

3.3.6 IDS

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

3.3.6.1 Metody detekce

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

daného útoku v databázi signatur. Obvykle se tato metoda omezuje pouze na inspekci jediného datového paketu, a je tedy snadno oklamatelná.

2) *Stavová detekce vzoru - Rozšíření předchozí metody, které umožňuje analyzovat datový tok (např. TCP stream) a detekovat signatury i v případě, že jsou rozděleny do více paketů.*

3) *Dekódování protokolu - Systém nejprve detekuje používaný protokol komunikace mezi entitami a následně na něj aplikuje pravidla definovaná v RFC (Request for Comments) a identifikuje případné porušení těchto pravidel.*

4) *Heuristická analýza - Tato metoda využívá statistické vyhodnocování parametrů monitorovaného provozu. Takto se dají například snadno detekovat útoky typu port sweep.*

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

3.3.6.2 Architektura IDS

1) *Host-based IDS Senzory*

Host-based IDS hledají útoky na úrovni operačního systému počítače. Jsou to softwarové produkty, které jsou instalovány na tyto koncové stanice a umožňují proto okamžitě určit, zda došlo k útoku na daný počítač a zda byl úspěšný či nikoli a dokáží řadě útoků zabránit. Tyto systémy monitorují systémová volání, chybová hlášení, logy a administrátorem určené důležité soubory. Existují typy útoků, které jsou snadno odhalitelné pouze těmito systémy. Nevýhodou těchto

systémů je skutečnost, že chrání pouze koncové počítače a neposkytují ochranu pro celou síť, a také skutečnost, že nepodporují všechny operační systémy, a tudíž nemohou poskytovat ochranu pro heterogenní sítě.

2) *Network-based IDS Senzory*

   Tyto systémy monitorují všechny pakety v síti pomocí NIC (Network Interface Card) rozhraní v promiskuitním módu a porovnáním těchto paketů se signaturami detekují útoky. Umožňují tak chránit celou síť a díky "neviditelnosti" monitorovacího rozhraní jsou těžko zranitelné.

   Hlavní problém při implementaci těchto systémů je šířka pásma sledovaných linek či segmentů, která v současné době dosahuje řádově Gbit/s. Při překročení přenosové rychlosti monitorovacího rozhraní IDS systému dochází ke ztrátě paketů. Kapacita současných IDS systémů dosahuje 100Mbit/s a v nejnovějších verzích dosahuje rychlosti 1 Gbit/s.

   Další nevýhodou těchto systémů je nemožnost detekovat útoky v šifrovaném provozu, tudíž je vhodné umístit monitorovací rozhraní do segmentů, kde nejsou data kryptována.

3) *Dohledový systém IDS*

   Správu prvků systému IDS usnadňuje specializovaný dohledový software, který usnadňuje administrátorům IDS provádění vzdálené konfigurace IDS senzorů. Jednotlivé IDS senzory komunikují s dohledovou stanicí, předávají jí informace o realizovaných útocích. Dohledový systém umožňuje konfigurovat reakci IDS systému na určité typu útoků. IDS senzor je pak např. schopen provést reset TCP spojení, prostřednictvím kterého probíhá domnělý útok, nebo dynamicky aplikovat filtrovací pravidla na směrovač nebo firewall, a znemožnit tak nevhodné aktivity útočníka. Dohledová stanice je schopna upozornit na probíhající útok administrátora např. elektronickou poštou nebo zprávou na pager. Prostřednictvím tohoto softwaru se rovněž realizuje aktualizace databáze

signatur, která obsahuje charakteristiky známých útoků.

4) *Design sítí se systémy pro detekci neoprávněného průniku Network-based IDS je vhodné umístit zejména do hraničních částí počítačové sítě. Typické je doplnění firewallové ochrany systémem IDS, kdy firewall realizuje filtraci provozu dle nastavených pravidel a systém IDS monitoruje datový provoz, upozorňuje na útoky a případně spolupracuje s firewallem nebo hraničním směrovačem při eliminaci neoprávněné aktivity. IDS lze umísťovat do segmentu mezi směrovač do internetu a firewall, resp. mezi firewall a vnitřní část sítě, do demilitarizovaných zón, ke směrovačům zabezpečujícím vzdálený přístup uživatelů do podnikové sítě. Další zónou, kde lze s výhodou využít vlastností IDS, je rozhraní mezi produkční sítí a mezi sítí se stanicemi pro dohled a správu produkční sítě. Segmenty, ve kterých se nacházejí kritické aplikační a databázové servery, jsou dalším místem, kde lze s výhodou využít vlastností IDS.*

3.3.6.3 Shrnutí IDS

Důležitou součástí implementace IDS je pravidelné vyhodnocování informací zaznamenaných systémem (logů) a následné ladění konfigurace systému. Tato procedura významně snižuje množství falešných poplachů způsobených např. přílišnou citlivostí systému na aktivity, které mohou být v daném případě neškodné a souvisejí s normálním fungováním informačního systému.

Systémy pro detekci neoprávněného průniku využívají pro odhalení útoků různé metody, přičemž nejlepší výsledky lze dosáhnout se systémy implementujícími kombinaci více různých metod detekce. Kombinací síťových IDS a IDS umisťovaných přímo na serverech potlačíme nevýhody spojené s implementací jediného IDS systému, a dále tak zvýšíme zabezpečení jednotlivých subsystémů. Nedílnou součástí nasazení IDS musí být

i související organizační opatření, která zajistí pravidelné vyhodnocování informací získaných z IDS a následnou úpravu parametrů systému.[7]

3.3.7 IPS

Donedávna se mělo za to, že firewally a systémy detekce průniků (IDS) dostatečně chrání síť před kompromitováním viry, červy, spywarem atd. Proč to neplatí a jak revolučně mění přístup systémy prevence průniků (Intrusion Prevention Systems – dále jen IPS) bude představeno v následující kapitole.

3.3.7.1 Princip IPS

Optimální IPS by v sobě měli mít automaticky nastaveny tisíce filtrů pro blokování nekorektní komunikace v tom, čemu se říká "doporučená" konfigurace. Tyto filtry rozpoznají provoz, který je pokládán za škodlivý kdykoliv, za jakýchkoliv podmínek a v jakémkoliv prostředí. V optimálním případě administrátor tento systém pouze zapne, nakonfiguruje uživatelské jméno a heslo pro administrativní rozhraní a připojí datové kabely. Od tohoto okamžiku by měl být systém plně funkční, blokovat útoky a chránit zranitelné systémy před kompromitováním. Žádné „Walk before Run“, či jinak nazývané používání v IDS režimu před přepnutím do IPS režimu, které je spojené s náročným hledáním false positiv. Před uvedením rozumného IPS do plnohodnotného provozu by nemělo být třeba žádné konfigurace, korelace, integrace nebo ladění čehokoliv. Pokud je to možné, měl by IPS systém poskytovat i karanténní činnost. Pod karanténní činností myslíme schopnost nejen zablokovat šíření škodlivého kódu, ale i aktivně pracovat se stanicí, která šíření tohoto kódu realizuje. Například vhodnou formou informovat uživatele lokální sítě, jehož stanice je nakažena, zablokovat port příslušné stanice na přepínači, přepnout port přepínače do karanténní virtuální sítě a také se postarat o doručení příslušných „léčebných“ procedur. To vše pokud možno bez zásahu administrátora, automaticky. Dále by měl mít optimální IPS efektivní systém aktualizace svých filtrů, které by se měli okamžitě, tím myslíme zase bez ladění,

[7] *Systémy pro detekci neoprávněného průniku – Časopis IT Systems – 7-8 2003* [online]. c2003, poslední revize 07.2003 [cit. 2010-01-02]. Dostupné z <http://www.systemonline.cz/clanky/systemy-pro-detekci-neopravneneho-pruniku.htm>.

nasazovat do činnosti. V neposlední řadě by měl být systém certifikovaný, že opravdu provádí to, co se od něho očekává. Základní certifikační autoritou je v případě IPS stejně jako firewallů ICSA Labs.

3.3.7.2 Filtry v IPS

Tvůrce IPS filtrů navrhuje filtry tak, aby neměly falešná pozitiva, nezhoršovaly výkon a byly odolnější vůči útočníkům, kteří se speciálně zaměřují na vyhnutí se detekci. Tento úkol přinesl velkou změnu ve filozofii přístupu, která byla tradičně přijímána v oblasti IDS. Navíc tento úkol vyžaduje nebývalý výkon a flexibilitu u prevenčního zařízení i filtrovacího jazyka.

Při psaní filtrů pro blokování musí být dodržena dvě pravidla:

1. *Žádná falešná pozitiva. Nikdy, za žádných okolností nesmí IPS blokovat legitimní provoz. Toto pravidlo má vždy nejvyšší prioritu.*
2. *Žádná falešná negativa. Nenechte projít útok, ani když se útočník intenzivně snaží vyhnout detekci. Toto má vysokou prioritu.*

Tvůrce filtrů musí mít stále na paměti tato dvě pravidla a jejich relativní prioritu. Klíčový rozdíl v přístupu k psaní signatur mezi IPS a IDS spočívá ve vzájemném pořadí těchto dvou cílů. Umění tvorby filtrů pro blokovací zařízení spočívá v co největším zobecnění logiky detekce tak, aby bylo dosaženo pravidla 2, bez porušení pravidla 1.

Nejprve je nutno definovat některé pojmy. Slovo signatura se používá pro popis logiky detekcí; to znamená shromažďování testovacích kritérií používaných k oddělení útočného provozu od normálního. Obecně je signatura spíše abstraktní pojem, který popisuje klasifikační algoritmus, ale nic neříká o způsobu, jakým bude reagováno na kladnou identifikaci útoku. Protože IDS pouze identifikují útoky, ale nijak na ně nereagují, používá se slovo signatura pouze v souvislosti s IDS.

Na druhou stranu slovo filtr se používá v souvislosti s logikou detekce v kombinaci s předpokládanou blokovací akcí. Filtry obsahují „pruning“, neboli odstraňování něčeho z toku provozu. Výraz filtrování se obecně používá v souvislosti s firewally,

protože firewally aktivně odstraňují vybrané typy paketů z celkového toku. Nicméně "inteligence" stojící za filtrováním firewally je tradičně základní, založená z větší části na číslech portů a typech protokolů. Proto nemá příliš smysl diskutovat o "logice detekce" nebo "signaturách", které používá určitý filtr firewallu.[8]

3.3.7.3 Karanténa v IPS

Jedna z hlavních výhod IPS oproti IDS je schopnost reagovat i na interního útočníka. Pokud dojde ke chtěnému či nechtěnému útoku z vnitřní sítě a napadení jedné z pracovních stanic, tak je systém IPS schopný hrozbu zastavit. Jakmile IPS zjistí šíření škodlivého kódu tak je daná pracovní stanice doslova odstřižena od intranetu a internetu, tím že je přesunuta do vytvořené VPN (viz kapitola 3.4.1.3), ve které se nachází pouze daná infikovaná stanice. Současně je upozorněn uživatel pracovní stanice a administrátor. Veškeré tyto úkony jsou provedeny ihned po detekci škodlivého kódu a naprosto automaticky.

3.3.7.4 Shrnutí IPS

Vstup systémů prevence průniků na scénu promíchal vody terminologie a způsobil mnoho zmatku každému, kdo se zabývá bezpečností sítí. Ani jeden z existujících termínů – signatura a filtr – nepopisuje adekvátně schopnosti IPS, pokud byly interpretovány jako tradiční výbava IDS nebo firewallu. IPS dokáže, s podobnou inteligencí jako systém detekce průniků, velmi přesně odlišit útočný provoz od neškodného. Testovací kritéria IPS používaná k detekci každého útoku si jistě zaslouží název "signatura" ve významu flexibility a výkonnosti klasifikace. Navíc IPS aktivně odděluje závadný provoz z toku paketů, čímž okamžitě činí použitelným slovo "filtr". Nicméně zákazníci jsou z toho v rozpacích. Slovo signatura použité v popisu IPS si nikdo v duchu nespojí s blokovací schopností zařízení. Na druhou stranu ze slova filtr

[8] *Systémy prevence průniků (1) – jen detekovat nestačí* [online]. c2007, poslední revize 5.11.2007 [cit. 2010-01-03]. Dostupné z <http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&clanekID=331>.

mohou lidé odvodit, že "inteligence" tohoto zařízení se omezuje na jednoduchá pravidla používaná firewally.[9]

3.3.8 IDPS

Systémy IDPS (Intrusion Detection and Prevention System) jsou posledním evolučním krokem v řadě IDS a IPS. Kombinují v sobě funkce obou systému IDS a IPS a zákazník tedy nemusí řešit, které řešení je pro něj vhodnější. Systémy IDPS mají sice vyšší cenu, ale na druhou stranu poskytují komplexnější ochranu. Dokáží identifikovat a zastavit útok na úrovni sítě a zároveň i útok na úrovni aplikace. Veškeré útoky jsou potlačeny dříve, než můžou způsobit jakoukoliv škodu. Díky aktualizovaným databázím jsou tyto systémy schopny zastavit téměř 100% útoků. Jednotlivé specifikace systému IDPS nebudou představovány, jelikož se jedná o kombinaci systémů IDS a IPS, které byly představeny v předchozích kapitolách.

I přes teoretickou dokonalost systémů IDPS je třeba zdůraznit, že se jedná o jednu vrstvu zabezpečení, která pokryje pouze určitou část celého rizikového spektra. Pro mnoho firem bude určitě perspektivní investovat velkou část rozpočtu do certifikovaného IDPS, kdy bude zakoupeno kvalitní řešení. Nevýhodou jakékoliv velké investice je fakt, že velmi pravděpodobně poté nezbudou finance na zabezpečení zbytku lokální sítě.

Pokud má daná firma dostupné finance, tak systémy IDS, IPS či nejlépe IDPS nabízí jedny z nejlépe návratných investicí.

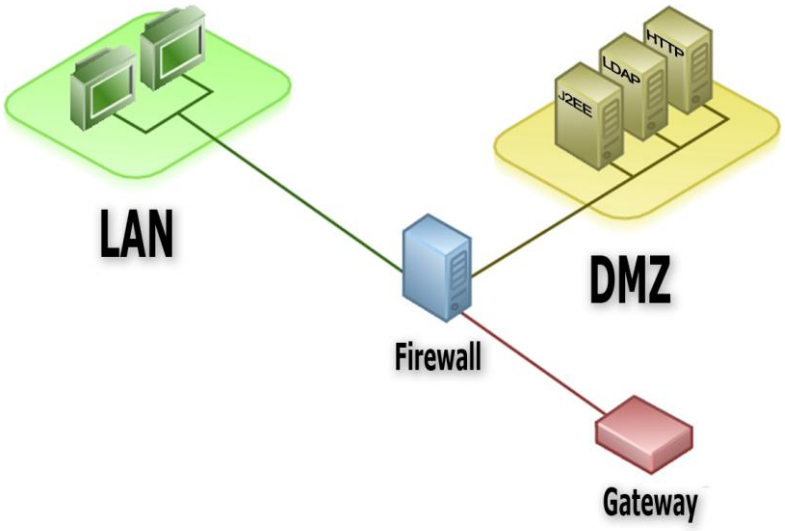
3.3.9 DMZ

DMZ je zkratkou pro anglický výraz demilitarized zone, který se nepřekládá do českého jazyka. Pojem DMZ označuje určitou část lokální sítě, která je z určitých důvodů oddělena od ostatních zařízení. Demilitarizované zóny (dále jako DMZ) jsou nejčastěji používány pro shlukování zařízení, která poskytují služby pro zbytek vnitřní

[9] *Systémy prevence průniků (1) – jen detekovat nestačí* [online]. c2007, poslední revize 5.11.2007 [cit. 2010-01-03]. Dostupné z <http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&clanekID=331>.

sítě (tedy lokální síť) nebo pro vnější síť. Princip DMZ tkví v tom, že zařízení v DMZ jsou přístupná z vnitřní i vnější sítě, ale klíčová úroveň přístupu je pro obě tyto sítě odlišná. DMZ tedy přímo představuje pravidlo, že zabezpečený systém by neměl mít přístup k nepotřebným službám.

Hlavním cílem DMZ je rozšíření celé struktury o další vrstvu zabezpečení a snížení rizika proti útokům. Na následujícím obrázku je zobrazen princip DMZ.



Obrázek 4 - DMZ, zdroj: http://docs.hp.com/en/5991-7435/ar01s04.html

Z obrázku je zřetelné, jak jsou odděleny klíčové síťové prvky od uživatelských stanic. V případě potenciálního úspěšného útoku je mnohem větší šance, že dojde k ohrožení pouhé části lokální sítě. Velmi často je pro rozdělení lokální sítě a DMZ používána dodatečná úroveň firewallu.

Pro provoz DMZ je vhodné používat samostatný server, který bude obstarávat kompletní správu celé zóny, přístupy atd. DMZ je možné provozovat i na společném serveru, kde jsou spuštěny další služby, ale z hlediska bezpečnosti a výkonu není tato možnost doporučována.

3.4 Wi-Fi

3.4.1 Definice a využití

Wi-Fi je standard pro lokální bezdrátové sítě (Wireless LAN, WLAN) a vychází ze specifikace IEEE 802.11 (viz Tabulka 1). Bezdrátové sítě nabízejí v principu podobné služby a flexibilitu jako sítě drátové. Je možné zapojovat do nich servery a jejich klienty, ale také je možné v nich vytvářet spojení peer-to-peer. Z hlediska funkčnosti a výsledku jsou, odhlédneme-li od dosahovaných přenosových rychlostí, ekvivalentní k sítím drátovým, kupříkladu ethernetu. Zásadně se samozřejmě liší ve své skutečné podstatě, v tom jak fungují. Wi-Fi technologie prošla několika zásadními updaty za uplynulé roky a dané fáze vývoje jsou značeny písmenkem za názvem specifikace IEEE 802.11. První verze byla 802.11a a vyznačovala se např specifikacemi jako WLAN v pásmu 5GHz a rychlost až 54 mbit/s.

Využití Wi-Fi se hlavně týká přenosných počítačů (v drtivé většině se jedná o notebooky). Popularita Wi-Fi se za posledních pět let několikanásobně zvýšila, což nebylo způsobeno nástupem převratné nové technologie, ale zásadním usnadněním domácí zábavy či pracovní náplně. Wi-Fi přinesla hlavně mobilitu a pohodlí, což jsou zásadní argumenty ve firemním prostředí. Usnadnění přenosu počítačů v rámci kancelářských prostor ať už za účelem předvádění libovolného obsahu/produktu v zasedací místnosti či kdekoliv jinde. Je přeci jenom vhodnější nabídnout klientovi možnost bezdrátového připojení než se zatěžovat s natahováním a zapojováním kabelu. Velká většina dnešních notebooků je nabízena s již zabudovaným Wi-Fi přijímačem a spousta firem používá WLAN v infrastruktuře.

3.4.2 Zabezpečení Wi-Fi

Problém bezpečnosti bezdrátových sítí vyplývá zejména z toho, že jejich signál se šíří i mimo zabezpečený prostor bez ohledu na zdi budov, což si mnoho uživatelů neuvědomuje. Dalším problémem je fakt, že bezdrátová zařízení se prodávají s nastavením bez jakéhokoliv zabezpečení, aby po zakoupení fungovala ihned po zapojení do zásuvky. Podle odhadů je více jak 60% firemních sítí otevřených anonymnímu

přístupu. Jejich správci pak buďto nevědí jak systém zabezpečit, případně se spoléhají na to, že nikdo nebude chtít jejich síť "využít".

Nezvaný host se může snadno připojit i do velmi vzdálené bezdrátové sítě jen s pomocí směrové antény, i když druhá strana výkonnou anténu nemá. Navíc většina nejčastěji používaných zabezpečení bezdrátových sítí má jen omezenou účinnost a dá se snadno obejít.

Různé typy zabezpečení se vyvíjely postupně, a proto starší zařízení poskytují jen omezené nebo žádné možnosti zabezpečení bezdrátové sítě. Právě kvůli starším zařízením jsou bezdrátové sítě někdy zabezpečeny jen málo. V takových případech je vhodné použít zabezpečení na vyšší síťové vrstvě, například virtuální privátní síť (kapitola 3.4.1.3). [10]

3.4.2.1 WEP

WEP (Wired Equivalent Privacy, česky soukromí ekvivalentní drátovým sítím) je původní zabezpečení Wi-Fi sítí a je součástí IEEE 802.11 standardu z roku 1999. Už z názvu je patrné, že cílem bylo poskytnout zabezpečení jaké je dostupné v drátových sítích. Protože se ale veškeré informace v bezdrátových sítích přenášejí volným prostorem, je snadné je odposlouchávat. Není totiž nutné se fyzicky drátem připojit k síti.

WEP používá proudovou šifrovací metodu RC4 pro utajení informaci a pro ověření jejich správnosti používá metodu CRC-32 kontrolního součtu.

Takzvaný 64bitový WEP používá 40bitový klíč, ke kterému je připojen 24bitový inicializační vektor a dohromady tak tvoří 64bitový RC4 klíč. 128bitový WEP používá 104bitový klíč, ke kterému je připojen 24bitový inicializační vektor a dohromady tak tvoří 128bitový RC4 klíč. Někteří výrobci bezdrátových zařízení poskytují i 256bitový WEP.

Bohužel je ale známo mnoho slabostí WEP zabezpečení, proto je dnes doporučováno používat silnější metody jako jsou WPA s AES a WPA2 (Wi-Fi Protected Access). Délka klíče není jedinou slabostí WEP zabezpečení. Společně s kolizemi

[10] *Wi-Fi - Wikipedie, otevřená encyklopedie* [online]. c2004, poslední revize 11.12.2009 [cit. 2010-02-10]. Dostupné z <http://cs.wikipedia.org/wiki/Wi-Fi>.

inicializačních vektorů a možností útoků pomocí zasílání pozměněných paketů, dělá z WEP velmi slabé zabezpečení.[11]

3.4.2.2 WPA a WPA2

WPA (Wi-Fi Protected Access, česky Wi-Fi chráněný přístup) vznikl jako reakce na vážné bezpečnostní nedostatky objevené v předchozím systému, jímž byl Wired Equivalent Privacy (WEP). Vznikl s cílem využít hardware podporující WEP, ale vhodnými doplňkovými mechanismy (především prací s klíči) eliminovat jeho slabá místa. Tento druh zabezpečení však nefunguje v tzv. ad-hoc sítích, ve kterých lze pro zabezpečení použít pouze WEP.

WPA implementuje velkou část standardu IEEE 802.11i. Vznikl jako dočasná náhrada WEP do doby, než bude dokončena specifikace 802.11i. WPA je navržen tak, aby pracoval se všemi Wi-Fi síťovými kartami, ale nemusí fungovat na nejstarší generaci přístupových bodů. Kompletní implementací standardu IEEE 802.11i je WPA2, což je následník WPA, který ale není podporován některými staršími kartami.

WPA2 implementuje povinné prvky IEEE 802.11i. Konkrétně přidává k TKIP a algoritmu Michael nový algoritmus CCMP - "Counter Mode with Cipher Block Chaining Message Authentication Code Protocol" založený na AES, který je považován za zcela bezpečný. Od 13. března 2006 je certifikace WPA2 povinná pro všechna nová zařízení, jež chtějí být certifikována jako Wi-Fi.

WPA a WPA2 poskytují kvalitní zabezpečení, pokud jsou dodržovány zásady základního zabezpečení jako např. vytváření a administrace bezpečných hesel (viz kapitola 3.3.2).

Součástí WPA i WPA2 je režim s předsdíleným heslem - PSK pre-shared key (označovaný také jako osobní režim) je navržen pro sítě v domácnostech a malých kancelářích (tzv. SOHO segment), které si nemohou dovolit náklady a složitost autentizačního serveru pro IEEE 802.1X - např. RADIUS server. Každý uživatel musí před vstupem do sítě zadat heslo obsahující 8 až 63 tisknutelných ASCII znaků nebo 64

[11] *Wired Equivalent Privacy - Wikipedie, otevřená encyklopedie* [online]. c2006, poslední revize 18.1.2010 [cit. 2010-02-10]. Dostupné z <http://cs.wikipedia.org/wiki/Wired_Equivalent_Privacy>.

šestnáctkových číslic. Pokud použijete ASCII znaky, hašovací funkce je zkrátí z původních 504 bitů (63 znaků po osmi bitech) na 256 bitů (používá také SSID). Většina operačních systémů umožňuje uložení hesla na uživatelském počítači, aby nebylo nutné jej opakovaně zadávat. Heslo musí být uloženo na všech přístupových bodech Wi-Fi sítě.

Bezpečnost zvyšuje použití funkce PBKDF2 (Password-Based Key Derivation Function) pro odvozování klíčů. Nicméně uživatelé často používají slabá hesla, která neodolají útokům hrubou silou zaměřeným na hádání hesel. Riziko tohoto útoku lze snížit použitím hesel kombinujících alespoň 5 spojených náhodných slov či obsahujících alespoň 14 zcela náhodných písmen. Maximální ochrana v tomto režimu vyžaduje klíč obsahující 54 náhodných písmen nebo 39 náhodných ASCII znaků. V praxi většinou postačí vyvarovat se krátkým a slovníkovým řetězcům.

Někteří výrobci spotřebních WLAN zařízení se snaží obejít slabou volbu hesla pomocí metody, která automaticky generuje a distribuuje silné klíče pomocí softwarového či hardwarového rozhraní používajícího externí metodu přidávání nového Wi-Fi adaptéru či zařízení do sítě. Tyto metody zahrnují stisknutí tlačítka (Broadcom SecureEasySetup a Buffalo AirStation One-Touch Secure System či AVM Fritz!Box Fon 7170, 7270) a zadání krátkého hesla prostřednictvím programu (Atheros JumpStart). Wi-Fi Aliance tyto metody standardizovala v programu nazvaném Wi-Fi Protected Setup (WPS, dříve Simple Config).

Některá zařízení podporují tzv. Mixed mode, kdy WLAN Access Point podporuje WPA a současně i WPA2 na jediném WLAN rozhraní, v některých případech umožňuje vytvořit i více, typicky 2 SSID bud přímo pro klienty (například mini router od FON.com - La Fonera, 2x SSID, 2 metody šifrování), v jiných případech např. pro WDS režim, kdy páteř je šifrována nezávisle na klientském signálu (např. Fritz!Box FON, i když obě SSID, páteřní i klientské, musí být shodné, tak každé může mít jinou metodu šifrování či klíče).[12]

[12] *Wi-Fi Protected Access - Wikipedie, otevřená encyklopedie* [online]. c2006, poslední revize 16.2.2009 [cit. 2010-02-18]. Dostupné z <http://cs.wikipedia.org/wiki/Wi-Fi_Protected_Access>.

3.4.2.3 VPN

Virtual Private Network (česky virtuální privátní síť) je prostředek k propojení několika počítačů prostřednictvím (veřejné) nedůvěryhodné počítačové sítě. Lze tak snadno dosáhnout stavu, kdy spojené počítače budou mezi sebou moci komunikovat, jako kdyby byly propojeny v rámci jediné uzavřené privátní (a tedy důvěryhodné) sítě. Při navazování spojení je totožnost obou stran ověřována pomocí digitálních certifikátů, dojde k autentizaci, veškerá komunikace je šifrována, a proto můžeme takové propojení považovat za bezpečné na rozdíl od slabě či vůbec nezabezpečené Wi-Fi sítě. [13]

VPN poskytují bezpečné spojení mezi klienty a zároveň se jedná o vhodnou alternativu, pokud jsou příliš vysoké náklady na řešení pomocí dedikovaného privátního komunikačního systému. Nejběžnější typy VPN ale nemusí znamenat jen propojení celých subsítí. VPN lze dále rozdělit či redukovat až na základní spojení typu uzel - uzel. Příkladem tohoto typu VPN je spojení uživatele se zabezpečenou aplikací, např. on-line bankovní službou, nebo zabezpečené kódované spojení mezi uživatelem a serverem při WWW obchodní transakci. Tento typ dynamických VPN typu uzel - uzel se dnes stává nejpoužívanějším v souvislosti s rozvojem elektronického obchodování. [14]

I přes veškeré výhody a silné stránky VPN je nezbytné, aby uživatel na konci VPN „tunelu“ měl dobře zabezpečený počítač. Pokud dojde k situaci, že daný uživatel bude mít infikovaný počítač, tak jakkoliv zabezpečené připojení neovlivní přenos infikovaných dat do firemní sítě nebo kamkoliv jinam kde ústí druhý konec VPN. K udržení bezpečného VPN spojení je tedy nutné aby klient či server nebyly infikováni.

---

[13] *Virtuální privátní síť - Wikipedie, otevřená encyklopedie* [online]. c2006, poslední revize 1.11.2009 [cit. 2010-02-19]. Dostupné z <http://cs.wikipedia.org/wiki/Virtu%C3%A1ln%C3%AD_priv%C3%A1tn%C3%AD_s%C3%AD%C5%A5>.

[14] VPN (2) – Internet versus plně privátní sítě [online]. c2003, poslední revize 8.1.2003 [cit. 2010-02-17]. Dostupné z < http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&clanekID=221>.

3.4.3 Zabezpečení Wi-Fi – shrnutí

Firemní či domácí Wi-Fi by měla splňovat několik následujících podmínek, abychom ji mohli klasifikovat jako zabezpečenou:

Základní úroveň zabezpečení

1) Deaktivované SSID – *Zablokování vysílání SSID sice porušuje standard, ale je nejjednodušším zabezpečením bezdrátové sítě pomocí jejího zdánlivého skrytí. Klienti síť nezobrazí v seznamu dostupných bezdrátových sítí, protože nepřijímají broadcasty se SSID. Bohužel při připojování klienta k přípojnému bodu je SSID přenášen v otevřené podobě a lze ho tak snadno zachytit. Při zachytávání SSID při asociaci klienta s přípojným bodem se používá i provokací, kdy útočník do bezdrátové sítě vysílá rámce, které přinutí klienty, aby se znovu asociovali.*[15]
2) MAC filter - MAC je jedinečný identifikátor každého síťového zařízení, který u jakýchkoli dvou zařízení není stejný (vyjma klonování MAC adres programy). MAC filter tedy povolí připojení na router jen MAC adresám, jež jsou autorizovány. Popřípadě opačně, že zablokuje přístup MAC adresám, které jsou zapsány v seznamu. V případě, že je používán pouze MAC filter jako zabezpečení, tak data putují sítí nejsou nijak zabezpečená a k jejich odposlechu není zapotřebí být připojen v dané síti. Součástí každého paketu je MAC adresa routeru a síťové karty počítače. V kombinaci s tím, že MAC adresu síťové karty si lze softwarově změnit je útok na danou síť otázkou chvilkového odposlechu bežného síťového provozu.
3) WEP - Bez ohledu na to, že WEP je "prolomitelný" je tato ochrana velmi důležitá. Aktivace WEP totiž zajistí nemožnost volného anonymního přístupu náhodným návštěvníkům do dané sítě.
4) SNMP tabulka - Tabulka IP adres, ze kterých je povolen SNMP management.

[15] Wi-Fi – (bezdrátový internet) – úvod, zabezpečení, struktura [online]. c2007, poslední revize 26.12.2007 [cit. 2010-02-11]. Dostupné z <http://mb.optimax.cz/2007/12/26/wirelless/Wi-Fi-bezdratovy-internet-uvod-zabezpeceni-struktura>.

Doporučovaná úroveň zabezpečení

1) WPA/WPA2 – Je důrazně doporučováno mít jakékoliv šifrování, přičemž WPA je bráno jako doporučené minimum. WPA2 je bráno jako zcela bezpečné, jelikož podporuje nové algoritmy a funkce zabezpečení.
2) VPN - *Pro maximální zabezpečení lze vybudovat Virtuální privátní síť mezi koncovými klienty (vybavenými SW pro VPN klienta) a VPN bránou, která je umístěna na metalické páteři mezi přístupovým bodem a vnitřní strukturou sítě. Tento kanál využívá šifrovaný protokol IPSec na třetí síťové vrstvě. Jedná se tedy o další vrstvu zabezpečení, nezávislou na předchozích. Takto zabezpečený systém snese nejpřísnější kriteria.* [16]
3) Vytváření a administrace hesel – hesla by měla být vytvářena v souladu s pravidly pro silné heslo a zároveň by měla být pravidelně kontrolována a eventuelně by mělo docházet ke změně hesel na pravidelné bázi.
4) 802.1X - Vzhledem k podobnosti systému přístupových bodů začali někteří výrobci nasazovat tento protokol pro vstupní zabezpečení do Wi-Fi sítí. Popis a funkce protokolu jsou popsány v kapitole 3.2.4.

3.5 Monitoring lokální sítě

Pojem monitoring lokální sítě popisuje využití systému, který neustále monitoruje počítačovou síť za účelem odhalení poruch, anomálního chování, sníženého výkonu a dalších faktorů, které mohou způsobit omezení či zastavení dané počítačové sítě.

Zatímco systém jako IDS monitoruje síť proti hrozbám z vnějšího prostředí, systém pro monitoring sítě je zaměřen na infrastrukturu dané sítě. Tyto systémy jsou schopny sledovat protokoly jako HTTP, HTTPS, SNMP, FTP, SMTP, POP3, IMAP, DNS, SSH, TELNET, SSL, TCP, ping, SIP, UDP a mnoho dalších. Veškeré monitorování probíhá v pravidelných intervalech, které nastavuje administrátor. Výsledkem jakéhokoliv monitoringu by měly být pravidelné reporty týkající se statusu

[16] *Jak na ochranu a zabezpečení Wi-Fi sítí | HW.cz* [online]. c2003, poslední revize 3.7.2003 [cit. 2010-02-11]. Dostupné z < http://hw.cz/ethernet/Wi-Fi/Wi-Fi_ochrana.html>.

dané sítě. Jakékoliv náhlé události by měly být vhodným způsobem (administrátor musí definovat způsob podávání varovných hlášení) hlášeny okamžitě.

V následujících kapitolách bude analyzováno několik vybraných programů vhodných pro monitoring sítí. Budou probrány jejich silné a slabé stránky spolu s vhodností využití pro určité segmenty trhu.

3.5.1 NetFlow

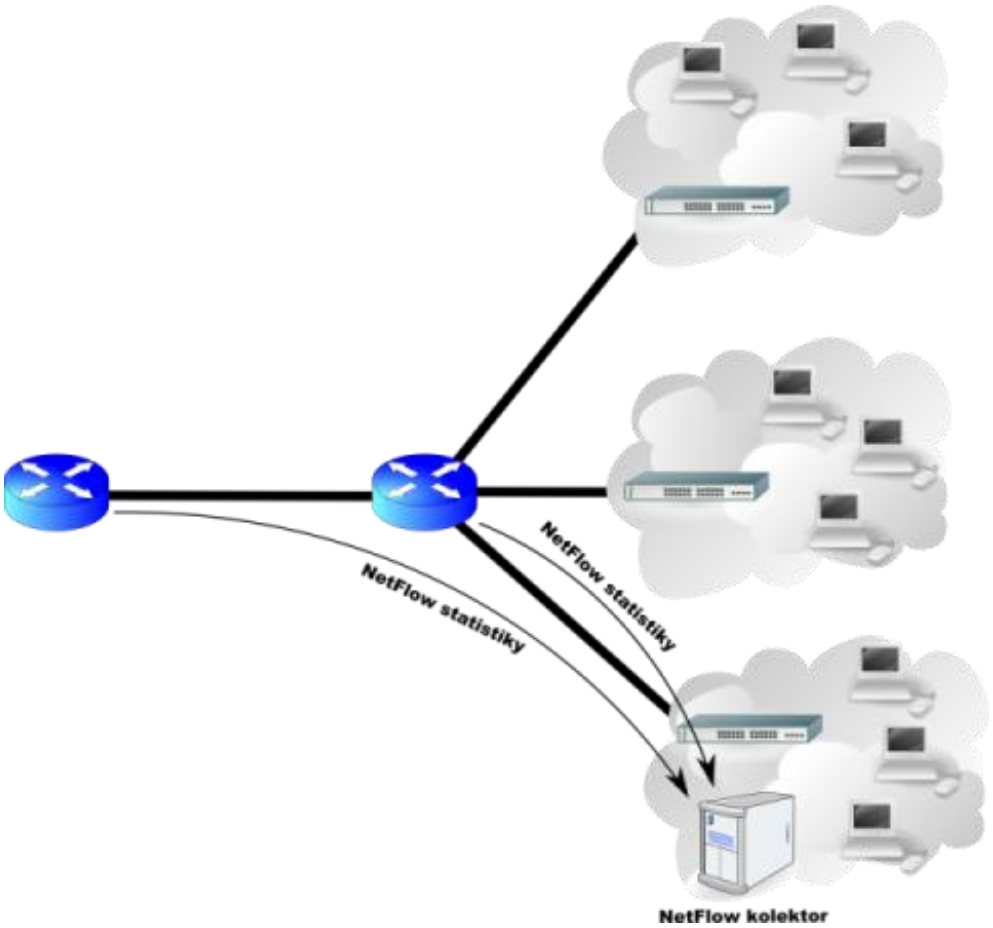
NetFlow je jedním z nejrozšířenějších současných standardů pro monitorování počítačových sítí.

NetFlow je otevřený protokol vyvinutý společností Cisco Systems, určený původně jako doplňková služba k Cisco směrovačům. Jeho hlavním účelem je monitorování síťového provozu na základě IP toků, které poskytuje administrátorům i manažerům podrobný pohled do provozu na jejich síti v reálném čase. Tok je v terminologii NetFlow definován jako sekvence paketů se shodnou pěticí údajů: cílová/zdrojová IP adresa, cílový/zdrojový port a číslo protokolu. Pro každý tok je zaznamenávána doba jeho vzniku, délka jeho trvání, počet přenesených paketů a bajtů a další údaje.

NetFlow architektura se typicky skládá z několika NetFlow exportérů a jednoho NetFlow kolektoru. NetFlow exportér je připojen k monitorované lince a analyzuje procházející pakety. Na základě zachycených IP toků generuje NetFlow statistiky a ty exportuje na NetFlow kolektor. NetFlow kolektor je zařízení s velkou úložnou kapacitou, které sbírá statistiky z většího počtu NetFlow exportérů a ukládá je do dlouhodobé databáze. Nad těmito daty obvykle běží aplikace, která je umí efektivně vizualizovat a generovat z nich přehledy v podobě grafů a tabulek, které umožňují jednoduše analyzovat monitorovaný provoz i běžnému uživateli.

Tradiční architektura - Tradiční architektura podle Cisco předpokládá na pozici NetFlow exportérů směrovače, které vedle své hlavní činnosti provádějí také výpočet NetFlow statistik. Tradiční architektura však trpí několika nevýhodami. Především se jedná o vysokou pořizovací cenu podobného zařízení, které brání jeho nasazení v malých a středních sítích. Výpočet NetFlow statistik také omezuje směrovací výkon celého zařízení, proto většina směrovačů s podporou NetFlow (s výjimkou těch

nejdražších) využívá na vstupu vzorkování, tzn., že se pro výpočet statistik využívá jen každý n-tý paket. Kromě snížené přesnosti měření omezuje vzorkování také pravděpodobnost odhalení bezpečnostních incidentů. Princip tradiční architektury je ukázán na následujícím obrázku. [17]

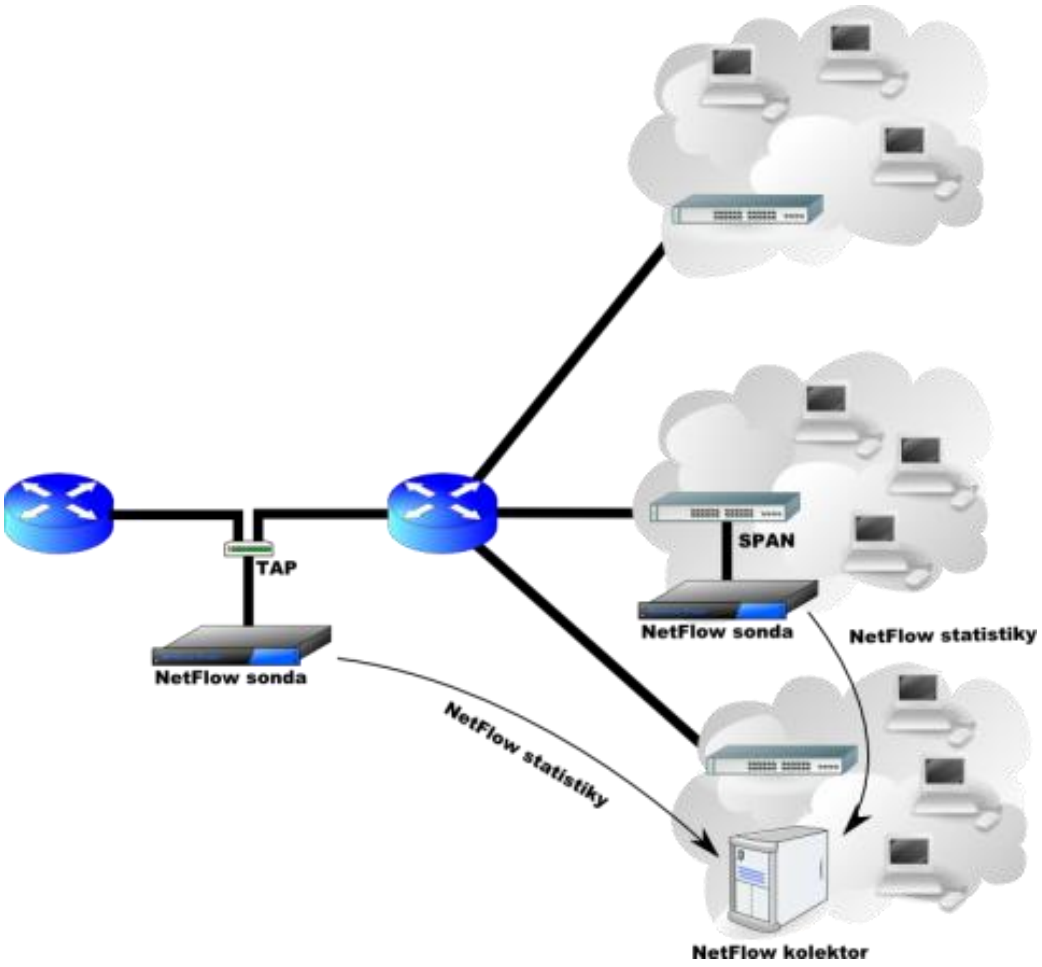


Obrázek 5 - Tradiční architektura NetFlow, zdroj: http://cs.wikipedia.org/wiki/Netflow

Moderní architektura – Moderní architektura byla vyvinuta za účelem snížení ceny řešení založených na tradiční architektuře. Hlavním prvkem moderní architektury jsou pasivní NetFlow sondy, což jsou zařízení na monitorování a následný export NetFlow statistik. Výhodou těchto sond je jejich jednoduchost a tedy i cena. Byly přímo vyvinuty, aby odstranily chyby z tradiční architektury. Tyto sondy lze připojit do jakéhokoliv bodu v síti a to transparentním způsobem. Funkce sond je čistě pasivní a

[17] *Netflow - Wikipedie, otevřená encyklopedie* [online]. c2008, poslední revize 26.3.2009 [cit. 2010-01-16]. Dostupné z <http://cs.wikipedia.org/wiki/Netflow>.

proudící data nijak nemodifikují a pouze zastávají monitorovací funkce. Další zásadní výhodou sond je fakt, že nasbírané statistiky o provozu jsou na kolektor odesílány vlastní linkou a nijak nezatěžují provoz normální linky a zároveň jsou na dané monitorované lince zcela neviditelné. Tento fakt velmi zlepšuje bezpečnost daného řešení, protože sondy jsou v podstatě neviditelné pro potencionální útočníky. Princip moderní architektury je ukázán na následujícím obrázku.



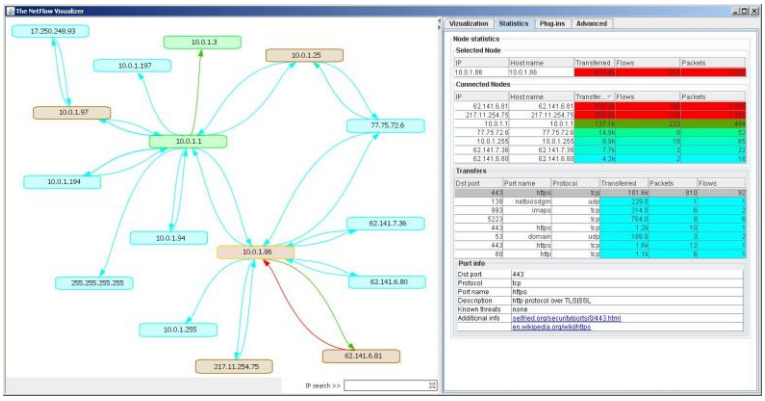
Obrázek 6 - Moderní architektura NetFlow, zdroj: http://cs.wikipedia.org/wiki/Netflow

3.5.1.1 Komerční řešení

Z různých nabízených řešení bylo vybráno FlowMon od firmy INVEA-TECH. Specifikace řešení FlowMon:

- založeno na moderní architektuře NetFlow (viz předchozí kapitola)
- využití sond, kolektorů a rozšiřujících modulů:

i. NetFlow Visualiser – modul ke grafickému zobrazení jednotlivých NetFlow toků. Tato metoda orientovaných grafů je vhodná pro analýzu úzkých či vytížených míst a následnou optimalizaci síťové infrastruktury. Obrázek 6 ukazuje využití NetFlow Visualiser modulu.



Obrázek 7 - NetFlow Visualiser modul, zdroj: http://www.invea-tech.com/cs/products/flowmon-plugins

ii. Nagios – modul k automatickému kontrolování. Prostřednictvím pravidelných dotazů je zjišťována dostupnost určitých služeb či zařízení a v případě zjištění specifického stavu dojde ke spuštění nadefinované akce jako např. e-mailová či SMS zpráva. Modul je schopný kontrolovat všechny možné zařízení či služby, které se vyskutují v dané lokální síti. Provoz modulu je náročný na konfiguraci a údržbu a je tedy vhodné vyškolení administrátora či využití outsourcingu.

- monitorování provozu na síti v reálném čase (i na linkách s propustností 10 Gb/s)
- možnost plánování a monitorování QoS
- detailní sledování uživatelů a služeb – vhodné ke zvyšování pracovní efektivnosti zaměstnanců
- dlouhodobé uložení statistik o síťovém provozu – umožňuje vytvářet dlouhodobé analýzy síťového provozu
- rozpoznání anomálií jako jsou červi a DDOS útoky

- účtování a fakturace na základě přenesených dat – jedná se tedy o řešení, které je finančně dostupné i v malých firmách (pokud ovšem nevykazují abnormálně velký internetový provoz).
- česká lokalizace celého řešení – vzhledem k složitosti nastavení a údržby je česká lokalizace dosti zásadní výhoda (pokud ovšem firma neplánuje využít outsourcing)

Silné stránky řešení FlowMon:

- Kompletní řešení pro monitoring lokální sítě
- Dlouhodobé statistiky vhodné k analýze a následné optimalizaci
- Přehledné grafické rozhraní
- Účtování na základě přenesených dat

Slabé stránky řešení FlowMon:

- Pořizovací náklady
- Náklady na školení zaměstnanců či administrátorů

Řešení FlowMon od firmy INVEA-TECH představuje klasický profil komerčního řešení. Jedná se o systém se správně zvoleným funkčním spektrem a přehledným grafickým rozhraním. Na druhé straně jsou zde nemalé pořizovací náklady spolu s časem, který zabere implementace celého systému a vyškolení zaměstnanců. V případě, že by došlo ke kompletnímu outsourcingu tak bude mít daná firma celé řešení na klíč, ale bude se jednat o vyšší pravidelný finanční náklad.

3.5.2 Wireshark

Počítačová aplikace Wireshark (dříve Ethereal) je protokolový analyzer a paketový sniffer. Mezi jeho nejčastější použití patří analýza a ladění problémů v počítačových sítích, vývoj software, vývoj komunikačních protokolů a studium síťové komunikace.

Wireshark nabízí velice podobné funkce jako tcpdump, navíc však obsahuje mnohem větší počet (stovky) analyzerů komunikačních protokolů a formátů (anglicky

dissector), grafické uživatelské rozhraní a mnoho možností uspořádání a filtrování zobrazených informací. Aplikace umí přepnout síťovou kartu do promiskuitního režimu a díky tomu dokáže zachytávat veškerou komunikaci na připojeném médiu.[18]

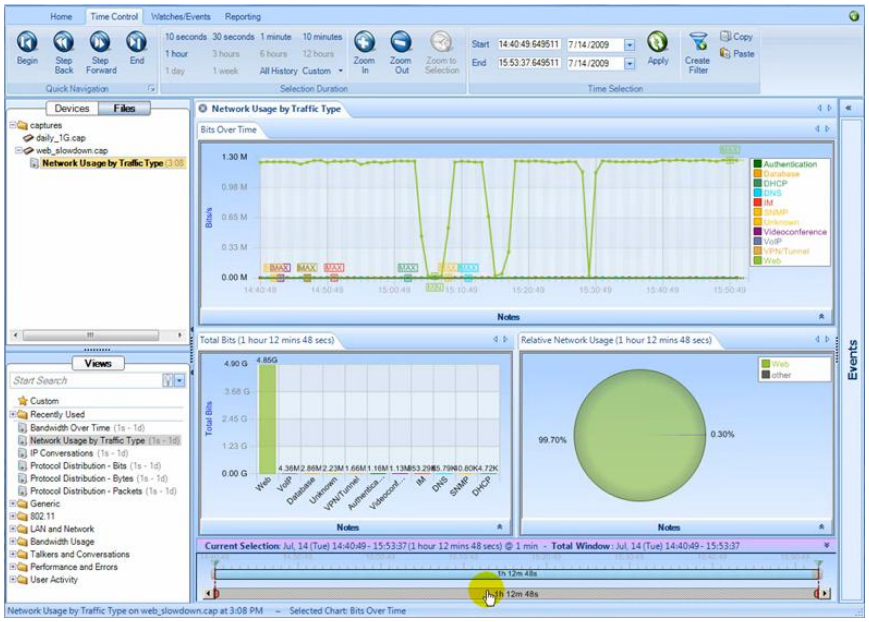
Wireshark je naopak od NetFlow uvolněný pod GNU General Public License a je tedy zdarma. Je to multi-platformový nástroj, který umí operovat na operačních systémech jako Windows, Linux, Solaris, BSD, Mac OS.

Specifikace řešení Wireshark:

- Multi-platformová kompatibilita
- Podpora obrovského množství protokolů – možnost monitorovat téměř cokoliv
- detailní sledování uživatelů a služeb – vhodné ke zvyšování pracovní efektivnosti zaměstnanců
- Vyvíjen pod GNU General Public License – volně šiřitelný
- Možnost zaznamenávat statistiky provozu a vytvářet analýzy
- Velmi detailní možnosti konfigurace
- Možnost využití rozšiřujících modulů

i. CACE Pilot® od firmy CACE technologies – komerční modul, který umí zpracovat výstupní data z Wiresharku a výsledky prezentovat ve více uživatelsky přívětivé formě. CACE Pilot umožňuje dlouhodobou analýzu provozu sítě a vytváření profesionálních reportů. Modul zároveň umožňuje sledování specifických protokolů a v případě, že dojde k nějaké změně tak je realizována nakonfigurovaná akce jako e-mail či SMS. Modul CACE Pilot představuje vylepšení Wiresharku na úroveň manažerskou, kdy má administrátor k dispozici velmi silný nástroj pro sledování celé sítě a zároveň je schopen sledovat dlouhodobé trendy, hledat slabá místa a eventuelně celou síť optimalizovat dle potřeb. Obrázek 8 ukazuje uživatelské prostředí CACE Pilot.

[18] *Wireshark - Wikipedie, otevřená encyklopedie* [online]. c2006, poslední revize 21.9.2009 [cit. 2010-01-21]. Dostupné z <http://cs.wikipedia.org/wiki/Wireshark>.



Obrázek 8 – CACE Pilot modul, zdroj:
http://www.cacetech.com/products/cace_pilot.html

Silné stránky řešení Wireshark:

- Volně šiřitelný
- Na domovské stránce jsou k dispozici video tutoriály, které mohou pomoct s prvními kroky konfigurace a použití
- Množství podporovaných protokolů
- Multi-platformová kompatibilita
- Velmi široké možnosti konfigurace
- S použitím modulu CACE Pilot se jedná o komplexní monitorovací a reportovací nástroj pro správu sítě

Slabé stránky řešení Wireshark:

- V základní verzi se jedná spíše o nástroj vhodný k hledaní slabých míst než komplexní nástroj jako komerční řešení FlowMon
- Pořizovací cena modulu CACE Pilot je v nejnižší verzi 1295$ což je zhruba 25.000Kč.
- Dobrá konfigurace Wiresharku vyžaduje čas a pokročilé znalosti daného administrátora

Wireshark jako samostatná aplikace je spíše vhodný pro vývojáře a výrobce různých síťových doplňků. Funkční spektrum je obrovské a Wireshark je skvělý nástroj pro odhalování jakýchkoliv vetřelců v síťovém provozu či detailní analýzu provozu jednotlivých počítačů. Pro dlouhodobé monitorování síťového provozu je dobré zakoupení licence na CACE Pilot k Wiresharku a uživatel či firma dostane nástroj, který se plnohodnotně vyrovná profesionálnímu řešení FlowMon (viz předchozí kapitola).

3.5.3 Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer (dále jen MBSA) je volně šiřitelný program, který je ke stažení na webových stránkách firmy Microsoft. Jedná se tedy o produkt, který je výhradně určen pro programy a operační systémy (nejstarší podporovaný operační systém je Windows XP) Microsoft. Na rozdíl od monitorovacích programů zmíněných v předchozích 2 kapitolách (3.5.1 a 3.5.2) je MBSA zaměřen na monitorování a analýzu zabezpečení počítačů, které jsou připojeny k lokální síti. Program umožňuje administrátorovi, aby z jakéhokoliv počítače na dané lokální síti provedl analýzu vybraných počítačů.

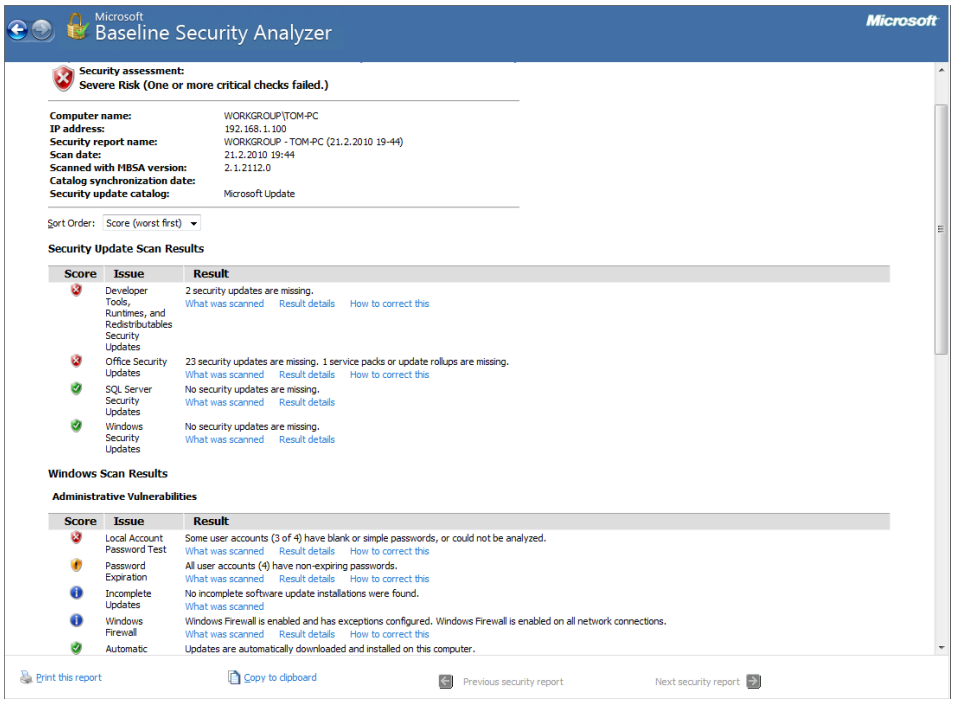
MBSA kontroluje následující:

- *vypršení platnosti hesel*
- *typ systémového souboru*
- *zda je zapnuta funkce Autologon*
- *zda používáme účet Guest*
- *restrikci anonymního uživatele*
- *počet administrátorských účtů*
- *prázdná nebo jednoducá hesla*
- *zda nejsou spuštěny zbytečné služby*
- *vytváří seznam sdílených složek*
- *zda je zapnut auditing*
- *chybějící Hotfix a Service Packs*

Dále jsou předmětem zájmu MBSA servery Microsoftu: IIS, SQL a desktopové aplikace. Kontrola chybějících balíčků Hotfix a Service Packs probíhá pomocí internetu. MBSA si ze serveru Microsoftu stáhne soubor s příponou XLS, v němž je

obsažen seznam opravných balíčků. Seznam pak porovná se skutečným stavem v konkrétním počítači (nebo počítačích) a zobrazí chybějící aktualizace. [19]

MBSA umožňuje provádět kontroly na jednotlivých počítačích či na libovolném počtu počítačů v dané síti. Výsledky kontroly jsou ukázány na následujícím obrázku.



Obrázek 9 - Výsledky MBSA kontroly

MBSA ve výsledcích testu zobrazí např. které Hotfixy chybí a jak může být daný problém napraven.

Hlavní výhodou programu MBSA je jednoduchost ovládání, přívětivé grafické rozhraní, rychlost s jakou jsou vykonávány dané kontroly a také fakt, že tento program je zcela zdarma ke stažení. Administrátor může pohodlně provádět pravidelné kontroly výše zmíněných bezpečnostních prvků a spolu s použitím konzole MMC Zásady skupiny (viz kapitola 3.3.3) lze průběžně optimalizovat bezpečnostní politiku.

I přes to, že MBSA je monitorovací nástroj, tak není přímým konkurentem řešení jako FlowMon či Wireshark, ale je skvělým doplňkem k jednomu z uvedených.

[19] HORÁK, Jaroslav. Bezpečnost malých počítačových sítí. 1. vydání. Praha: Grada, 2003. 200 s. ISBN 80-247-0663-6. Kapitola 4.2, Co MBSA kontroluje, s. 89

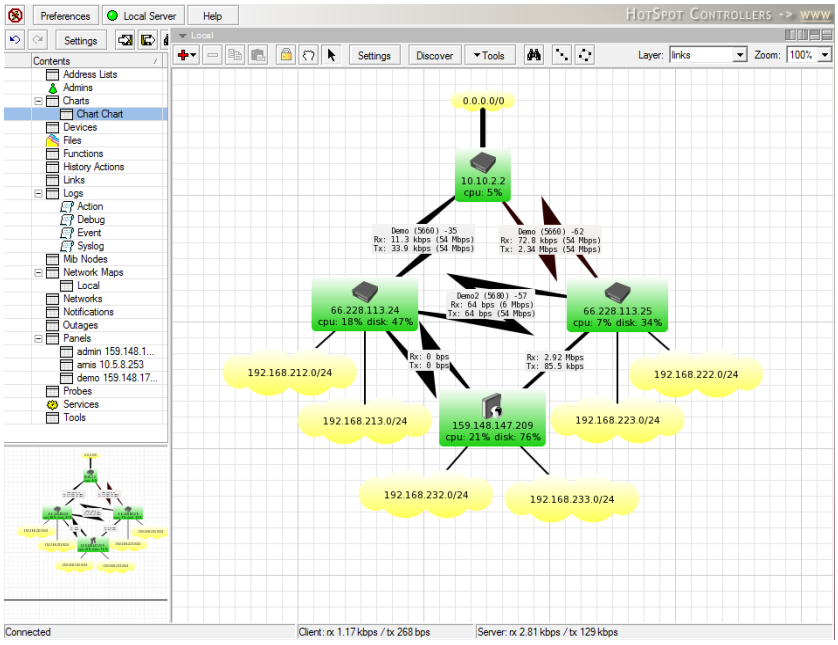
3.5.3 The Dude

The Dude je monitorovací program od společnosti MikroTik. Jeho hlavní funkce je monitorování dostupnosti síťových služeb.

Specifikace programu The Dude:

- Program je zdarma ke stažení
- Automatické mapování sítě a následné vytvoření schématu
- Objeví zařízení jakéhokoliv typu či značky
- Monitoring zařízení
- Notifikace při definované podmínce
- Umožňuje graficky upravovat vytvořené síťové schémata
- Jednoduchá a rychlá instalace i použití
- Přímý přístup ke vzdálené správě zařízení
- Podporuje vzdálený Dude server a lokálního klienta
- Lze provozovat na Linux Wine, MacOS Darwine and Windows

Uživatelské rozhraní a schéma zkoumané sítě je ukázáno na následujícím obrázku:



Obrázek 10 – Rozhraní v The Dude, zdroj: http://www.mikrotik.com/thedude.php

Silné stránky programu The Dude:

- Volně ke stažení
- Rychlost analýzy

- Jednoduchost ovládání
- Přehlednost uživatelského rozhraní i schémat
- Široká kompatibilita

Program The Dude lze považovat za názorný příklad jednoduchého, plně a rychle funkčního softwaru. Program je vhodný jak pro analýzu a optimalizaci síťového schématu, tak i na monitoring celé lokální sítě.

3.5.4 SNMP

SNMP je jednoduchý, široce rozšířený a užitečný standardizovaný protokol, který slouží k získávání nebo nastavování hodnot na určitém zařízení. Obdobou je například WMI od firmy Microsoft. Podporu SNMP má velká řada zařízení, například aktivní síťové prvky, počítačová čidla, tiskárny, přístupové body nebo pomocí softwaru a ovladačů ji mohou získat osobní počítače a servery. Hodnoty můžeme získávat v pravidelném intervalu a ty pak jednoduše ukládat do databáze spolu s časem a následně vykreslit do grafu. Přehledně tak můžeme zobrazit třeba vytížení procesoru, průběh teploty nebo datový tok na portu přepínače.

Protokol SNMP vyžaduje pro komunikaci dvě strany. Jednou entitou je správce (manager) a druhou agent. SNMP pracuje ve dvou režimech činnosti:

Správce posílá dotazy agentovi a přijímá odpovědi. Hodnoty tedy může získávat i více správců a mohou se ptát kdykoliv.

Agent zasílá oznámení (trapy) na adresu správce. V nějakých definovaných situacích (překročení nějaké hodnoty nebo i v pravidelném intervalu) odesílá agent jednomu správci hodnoty.

SNMP používá pro komunikaci UDP protokol, díky čemuž je velmi rychlé, ale může dojít ke ztrátě (nedoručení) zasílané informace (paketu). Od verze 2 je implementována kontrola doručení, takže ke ztrátě by nemělo dojít. Standardně se používá port 161 (SNMP) na straně agenta (pro dotazy) a port 162 (SNMPTRAP) na straně serveru (pro trapy). Klient, který posílá dotaz, zvolí dynamický port, z kterého

posílá dotaz na port 161. Agent odpovídá z portu 161 na dynamický port klienta. V praxi je pro každý dotaz použit jiný dynamický port.[20]

Funkce SNMP používá např. již zmiňovaný monitorovací program The Dude (viz kapitola 3.5.3). Vzhledem k tomu, že používání SNMP nezatěžuje komunikační pásmo, tak je program vhodný k testování propustnosti dané sítě a řízení toků. Obsluha SNMP bohužel vyžaduje pokročilé administrátorské znalosti a tak je využití SNMP vhodné spíše pro střední a velké firmy.

[20] *SNMP – Simple Network Management Protocol < články -> SAMURAJ-cz.com* [online]. c2006, poslední revize 20.12.2006 [cit. 2010-02-07]. Dostupné z <http://www.samuraj-cz.com/clanek/snmp-simple-network-management-protocol/>.

4 Možnosti řešení pro malé firmy

Na základě informací v literární rešerši bude v následujících podkapitolách sestaven návrh optimálního zabezpečení lokální sítě včetně monitoringu. Tento návrh nelze brát jako absolutní, protože v současné době není možné vytvořit dokonale bezpečný systém. Je pouze otázkou za jak dlouho lze daný systém prolomit. Výsledný návrh bude obsahovat nejvhodnější konfigurace (hlavně z hlediska poměru cena/výkon), různé doporučení a praktické postupy.

Následující podkapitoly budou vzhledem k přehlednosti strukturovány stejně jako hlavní podkapitoly literární rešerše.

4.1 Zabezpečení na hardwarové úrovni

Základním kamenem celé lokální sítě je její infrastruktura. Rozložení jednotlivých prvků ovlivňuje kvalitu a dostupnost poskytovaných služeb. Servery, zálohovací zařízení a záložní zdroje by měly být umístěny v nejméně frekventované místnosti, která by měla být uzamykatelná. Fyzický přístup k těmto klíčovým prvkům by měl být omezen pouze pro kvalifikované osoby. Rozmístění kabelových přípojek by mělo být v každé místnosti, kde lze pracovat a v lehce nadbytečném množství. Kabelové přípojky by neměly být na místech, kam může mít přístup i neznámý návštěvník, který by se mohl bez dozoru připojit k lokální síti.

UPS by mělo být standardním prvkem v jakékoliv lokální síti. Ve většině firem je využití UPS pro pracovní stanice nadbytečné, ale pokud pracovní náplň zaměstnance(ů) vyžaduje vysokou garantovanou dostupnost služeb, tak je využití UPS nezbytné. Servery a všechny ostatní důležité síťové prvky by měly být chráněny před výkyvy a výpadky elektrického napětí prostřednictvím UPS. Pro potřeby velmi malých firem můžou stačit i low-end řešení za nejnižší ceny. Pro potřeby malé až střední firmy je vhodné zvolit řešení, které nabízí pokročilejší funkce pro správu a monitorování. Vhodným zástupcem této kategorie je např. zmiňovaný model APC Back-UPS RS 800.

Využití síťových prvků s integrovanou ochranou závisí do velké míry na profilu dané firmy a na finančních prostředcích. Vzhledem k tomu, že podobné služby jsou dostupné i v podobě softwarových řešení tak byla vytvořena porovnávací tabulka 4. Cílem této tabulky bylo přehledně porovnat nabízené služby hardwarových a

softwarových bezpečnostních produktů. Porovnány byly produkty na stejné cenové hladině a zároveň produkty s nižší a vyšší cenou aby bylo možné najít pomyslný optimální produkt, který nabízí nejvíce služeb za adekvátní cenu.

Produkt/ Parametr	Kerio WinRoute Firewall	AirLive RS-3000	Netgear ProSafe VPN FW	ZyXEL ZyWALL USG 200	Cyberoam CR15i
Firewall	1	1	1	2	2
Antivir	1	1		2	1
Anti-spam		1		1	1
Anti-spyware					1
Web filtrace	1	1		1	1
Aplikační filtrace				1	1
QoS	1	1	1	1	1
IPS/IDS/IDPS		2		2	1
VPN	1	1	1	1	1
Individuální konfig.	1			1	1
Součet bodů	**6**	**8**	**3**	**12**	**11**
Cena (Kč)	15 214	10 866	8 239	17 185	11 901

Tabulka 4 – Porovnání softwarových a hardwarových firewallů

Vysvětlivky: U služeb jako firewall či antivir je možné získat certifikaci za kterou je udělen bod navíc. IPS a IDS jsou za jeden bod a IDPS jakožto kombinace obou je za 2 body. Softwarové řešení je vyznačeno modrou barvou a hardwarové řešení zelenou barvou.

Z tabulky 4 je možné vidět, že i produkty ve stejné cenové hladině se mohou zásadně lišit ve výbavě. Jediný zástupce softwarového řešení Kerio WinRoute Firewall nabízí sice plnohodnotný firewall se spoustou možných nastavení, ale oproti svým hardwarovým konkurentům nemá nic nenahraditelného. Produkty ZyXEL ZyWALL USG 200 a Cyberoam CR15i lze označit za výhodné produkty, které nabízí komplexní řešení za adekvátní cenu. ZyXEL ZyWALL USG 200 nabízí nejkvalitnější zabezpečení, které má IDPS a certifikovaný firewall a antivir. Za cenu zhruba 17 tisíc korun lze tedy získat celkové zabezpečení lokální sítě. Levnější Cyberoam CR15i nenabízí IDPS, ale pouze IPS a taktéž nemá certifikovaný antivir, ale je o zhruba 6 tisíc levnější. Lze tedy konstatovat, že Cyberoam CR15i je optimální produkt, který za cenu zhruba 11.000Kč nabízí dostatečné funkce pro kompletní zabezpečení a správu lokální sítě.

4.2 Zabezpečení na softwarové úrovni

V oblasti operačních systémů lze presentovat pouze několik doporučení. Pokud má daný uživatel dostatečné zkušenosti, tak je pro něj vhodnější používat operační systém na bázi Linux. V opačném případě je dobré zvolit operační systém firmy Microsoft a nejlépe verzi 7, která disponuje rychlým a přehledným grafickým rozhraním a zároveň má nejlepší zabezpečení ze všech systému od firmy Microsoft.

S ohledem na hierarchii v dané firmě by měly být vytvářeny uživatelské skupiny. Každý pracovník by měl mít přístup jen k datům, které potřebuje k vykonávání pracovní náplně. Přístup k datům lze i omezit na práva pro čtení či zápis což by mělo být využíváno. Uživatelské skupiny by měly zohledňovat i úroveň důvěry. Noví zaměstnanci či pracovníci ve zkušební lhůtě by měli mít minimální nutný přístup, který by jim měl být postupně rozšiřován.

Antivirový program by měl být nainstalován na každé pracovní stanici a bez ohledu na to, jestli je jiný antivirový program integrován v routeru nebo na serveru. Cílem je vytvoření víceúrovňové architektury, která je schopná odolat útoku zvenčí i zevnitř. Kvalitní antivirové programy mají více vyhledávacích motorů, což zlepšuje jejich schopnost identifikovat škodlivý kód. Mezi nejznámější výrobce antivirových programů patří např.: ESET, AVG, Norton, McAfee, F-Secure.

Do softwarové části zabezpečení patří bezesporu i firewall, ale samotné řešení firewallu bylo probráno v předchozí kapitole. Je samozřejmě možné zakoupit čistě softwarové řešení, ale z tabulky 4 bylo zřejmé, že výhodnější koupí představují routery, které mají v sobě integrovaný firewall a spoustu dalších bezpečnostních prvků. V případě dostupných finančních prostředků je možné pořídit i softwarový firewall aby byla vytvořena víceúrovňová architektura.

Systémy IDS/IPS/IDPS byly také zmíněny v předchozí kapitole v souvislosti s integrací v routerech. Jejich využití je v roli zabezpečení také velmi důležité. Jejich nasazení by mělo být provedeno s rozmyslem a nutnou znalostí jejich rozdílných specifikací a slabých míst. Nejlepší variantou je bezesporu IDPS, který kombinuje schopnosti IDS i IPS a je schopen zabezpečit firmu zvenčí i zevnitř. Systémy IDS či IPS naopak ke kompletnímu zabezpečení potřebují vhodné doplnění (firewall, antivir, monitorovací nástroj) aby byla firma zabezpečena oboustranně.

4.3 Zabezpečení Wi-Fi

Wi-Fi infrastruktura by měla korespondovat s infrastrukturou lokální sítě. Veškeré přístupové body by měly být umístěny s ohledem na optimální vzdálenost od uživatelů, kteří se připojují přes Wi-Fi. Je zbytečné, aby např. na jednom patře byly umístěny 2 přístupové body v rozích místností, když by celé patro optimálně pokryl jeden vhodně umístěný přístupový bod.

Pokud v dané firmě nedochází k nějakým častým přesunům s počítači tak by vhodné aby bylo vždy preferováno pevné kabelové připojení před Wi-Fi připojením. Pokud pracovník používá notebook většinu času na jeho/jejím pracovním stole, tak je vhodné instruovat tyto pracovníky, aby pro připojení k lokální síti využívali pokud možno kabel místo Wi-Fi.

Pro dosažení minimální úrovně zabezpečení je nutné mít aktivní a nakonfigurované následující prvky: MAC filtr, SNMP tabulka, WEP a zablokování vysílání SSID.

Pro dosažení optimální úrovně zabezpečení je nutné mít aktivní předešlé prvky a zároveň WPA a WPA2. Pro nadstandardní zabezpečení je možné vytvořit VPN pro jednotlivé uživatele. Základním předpokladem pro veškeré vyjmenované prvky je dodržování zásad pro vytváření a správu bezpečných hesel.

4.4 Monitoring lokální sítě

Nástroje pro monitorování lokální sítě by se, stejně jako operační systémy, daly rozdělit do dvou skupin. V první skupině jsou komerční produkty, které nabízí spoustu služeb, přívětivé uživatelské prostředí a jsou vhodné i pro dlouhodobý management lokální sítě. Na druhé straně jsou zde programy, které jsou více specializované, neposkytují tak široké služby, nemají natolik přehledné a přívětivé uživatelské prostředí, ale jsou zdarma. V následující tabulce jsou porovnány všechny řešení analyzované v kapitole 3.5.

Produkt/ Parametr	FlowMon	Wireshark	The Dude	MBSA
Monitorování sítě	X	X	X	
Monitorování zařízení	**X**[1]		X	
Plánování a monitorování QoS	X	X		
Detailní sledování protokolů	X	X		
Detailní sledování uživatelů	X	X		
Dlouhodobé statistiky	X	**X**[3]	X	
Detekce škodlivých kódů	X			
Platformová kompatibilita		X	X	
Grafické zobrazení struktury sítě	**X**[2]	**X**[3]	X	
Analýza uživatelské struktury				X
Analýza hesel				X
Monitoring aktualizací				X
Rozšiřitelnost	X	X		
Česká lokalizace	X			
Volně šiřitelný		X	X	X

Tabulka 5 - Porovnání monitorovacích nástrojů

Vysvětlivky: *1) Pouze s modulem Nagios*

2) Pouze s modulem FlowMon Visualiser

3) Pouze s modulem CACE Pilot, který není zdarma

Z tabulky 5 lze vyčíst, že jediné komerční řešení FlowMon nabízí nejširší sortiment služeb, včetně české lokalizace. Zakoupení dodatečných modulů přidává funkce pro monitorování zařízení a grafickou správu lokální sítě.

Prostřednictvím přímého porovnání nabízených služeb lze dojít k tomu, že kombinací volně šiřitelných programů jako Wireshark a The Dude lze dosáhnout téměř podobného funkčního spektra jaké nabízí FlowMon. Klíčovým nedostatkem může být absence české lokalizace, protože ne každý správce sítě má dostatečně pokročilé znalosti technické angličtiny. Je zřejmě, že kombinace dvou programů nemůže plně nahradit komplexně promyšlenou strukturu a funkce FlowMonu. Je také zřejmé, že úroveň nabízených služeb bude o nějaký stupeň nižší u volně šiřitelných programů. Výhodou programů Wireshark a The Dude je jejich kompatibilita s ostatními operačními systémy a nejdůležitějším faktem je nulová pořizovací cena (pokud ovšem není zakoupen modul CACE Pilot). Výběr vhodného řešení by měl záviset na klíčových požadavcích dané firmy. Pokud např. bude požadavek na program v českém jazyce tak

není jiné alternativy než FlowMon a pokud by byl např. požadavek pro provoz na Linuxovém operačním systému, tak jedinou alternativou je Wireshark, The Dude nebo kombinace obou. Pokud jsou klíčovým faktorem finanční prostředky tak je bezesporu nejvýhodnější vyzkoušet Wireshark, The Dude nebo kombinaci obou.

Program MBSA je poněkud odlišný od výše uvedených. Je přímo specifikován na analýzu uživatelských účtů a hesel. Zároveň lze s tímto programem kontrolovat zda-li je na každém počítači na lokální síti nainstalován nejnovější aktualizační balíček či Service Pack. Jedná se tedy o monitoring odlišných oblastí zabezpečení. MBSA je volně stažitelný a měl by tedy být součástí sady monitorovacích nástrojů každého administrátora.

Pokud vezmeme v potaz kombinaci programů Wireshark, The Dude a MBSA, tak lze za nulovou cenu získat komplexní řešení na monitorování lokální sítě a jejích součástí jako jsou zařízení, uživatelé, uživatelské účty atd. Řešení FlowMon má svoje nezpochybnitelné výhody a je vhodné pro střední a velké firmy nebo takové firmy, které mají specifické klíčové požadavky jako např. česká lokalizace či možnost kompletního outsourcingu celého monitorování lokální sítě.

5 Analýza bezpečnostní situace ve vybrané firmě

5.1 Představení firmy – pracovní náplň

Firma Crazy Tomato s.r.o. byla založena 8. července 2005. Hlavním předmětem podnikání je reklamní činnost a marketing v oblasti mobilních telefonů. Firma současně poskytuje různé služby jako je hromadné rozesílání SMS zpráv či informování občanů o různých kalamitách také prostřednictvím SMS zpráv.

V současné době zaměstnává 15 lidí, přičemž stálých zaměstnanců je 11 a ostatní jsou externisté. Firma má svojí jedinou kancelář v Praze. V této kanceláři pravidelně pracuje 10 lidí, přičemž jeden člověk nepravidelně dochází na několik dní v týdnu.

Veškerá počítačová bezpečnost je firmě obstarávána externím IT specialistou, který do firmy dochází pouze na požádání, ale pomocí vzdáleného přístupu pravidelně kontroluje síťový provoz.

5.2 Bezpečnostní analýza

Hlavní kancelář sestává ze tří pater, přičemž ve spodním patře pracuje 6 lidí, ve druhém patře 3 lidé a v posledním patře 2 lidé. Na každém patře jsou v dostatečném množství rozmístěné síťové porty. V posledním patře se nachází zasedací místnost, kam zhruba jednou za dny chodí návštěva. V druhé místnosti v posledním patře se nachází pracovní místa pro 2 zaměstnance a zároveň hlavní centrum síťového provozu. Toto centrum se skládá z 2 serverů, přičemž jeden z nich je profesionální komerční řešení od firmy HP s označením Proliant 110 ML. Tento server je provozován s operačním systémem Windows Server 2003, poskytuje centrální úložiště dat a slouží jako internetová brána pro celou lokální síť. Na hlavním serveru jsou také provozovány další bezpečnostní služby jako např. ESET NOD. Na druhém serveru je provozována pouze firewall s označením Endian Firewall verze Community, která je zdarma. Tento firewall má velmi podrobné možnosti nastavení a disponuje nepřeberným množstvím modulů. V samotném firewallu je integrován systém IDS i IPS, které jsou oba aktivní. Dalším klíčovým prvkem je externí záložní disk Western Digital, na který jsou pravidelně ukládány veškeré důležité data. Závěrečným doplňkem je UPS od firmy Belkin

s kapacitou 1500VA. Tato kapacita je plně dostačující pro záložní provoz obou serverů i záložního disku. Pokud dojde k výpadku elektrického proudu, tak budou oba servery schopné uložit veškeré nastavení a samostatně se vypnout.

Každý zaměstnanec disponuje vlastním počítačem, z čehož pouze dva jsou klasické pracovní stanice a zbytek představují notebooky. Dva notebooky jsou poněkud zastaralejšími typy, ale jejich výkon je pro kancelářské aplikace stále dostatečný. Zhruba čtyři zaměstnanci používají kabelové připojení k internetu a zbytek používá Wi-Fi. Nejpoužívanějším operačním systémem jsou Microsoft Windows XP. Na dalších počítačích se vyskytují operační systémy Windows Vista, Linux Ubuntu a MacOS, vždy po jednom exempláři. Na všech operačních systémech Windows jsou nainstalovány antivirové programy ESET NOD. Na operačních systémech Ubuntu a MacOS nejsou antivirové programy nainstalovány, jelikož škodlivé kódy na těchto systémech nejsou příliš rozšířené.

V následující tabulce je ukázán bezpečnostní antivirový report pro celou lokální síť za posledních 7 měsíců.

Pořadí	Typ hrozby	Počet	První výskyt
1	INF/Autorun virus	4	5.10.2009 13:07
2	a variant of Win32/Kryptik.CKL trojan	3	15.2.2010 17:21
3	a variant of Win32/Kryptik.CNQ trojan	3	21.2.2010 3:48
4	Win32/Oficla.CT trojan	3	27.1.2010 9:06
5	a variant of Win32/AutoRun.KS worm	2	5.10.2009 13:07
6	a variant of Win32/Kryptik.CIW trojan	2	12.2.2010 15:55
7	a variant of Win32/Kryptik.CJT trojan	2	17.2.2010 10:44
8	a variant of Win32/Spy.Zbot.VM trojan	2	28.10.2009 10:18
9	Win32/Oficla.EH trojan	2	6.3.2010 18:21
10	Win32/TrojanDownloader.Bredolab.AN trojan	2	16.2.2010 21:16
11	Win32/TrojanDownloader.FakeAlert.GU trojan	2	12.10.2009 20:08
12	a variant of Win32/Injector.AXS trojan	1	23.2.2010 7:52
13	a variant of Win32/Kryptik.ASA trojan	1	13.10.2009 14:15
14	a variant of Win32/Kryptik.ATY trojan	1	12.10.2009 17:59
	Ostatní (15)	15	
	Součet všech výskytů	**45**	

Tabulka 6 - Bezpečnostní antivirový report z ESET NOD

Z tabulky lze vidět, že celkový počet výskytů není příliš velký, ale zhruba jednou za týden dojde k několika výskytům škodlivého kódu.

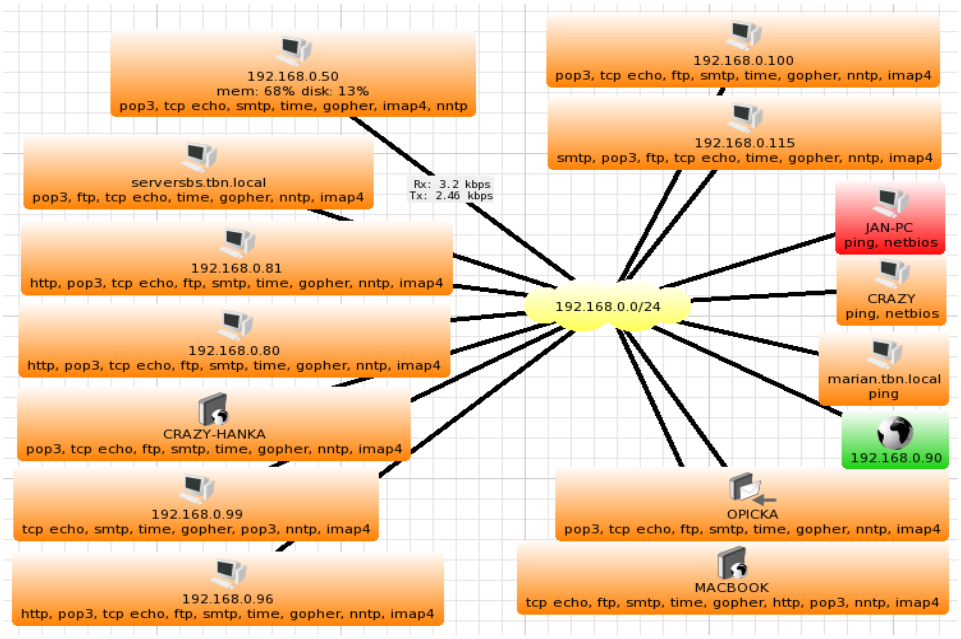
Pouze jeden zaměstnanec je přihlášen do domény v Active Directory a zbytek používá běžné uživatelské účty a skupiny. Uživatelské skupiny nemají nijak definovaná přístupová práva.

Provozovaná Wi-Fi síť má přístupové body na každém patře. Wi-Fi síť byla až donedávna zabezpečena pouze prostřednictvím WEP. Z manažerského hlediska poskytoval tento protokol dostatečné zabezpečení, ale po několika urgencích ze strany administrátora byl odsouhlasen přechod na WPA. Tento krok znamenal pro zaměstnance nutnost naučit se několik nových postupů, ale samotné zabezpečení prostřednictvím WPA bylo nezbytným krokem. Protokol WPA2 bohužel není podporován na 2 starších noteboocích, takže jeho provoz není možný.

Dva zaměstnanci využívají VPN protokol pro občasnou práci z domova. Vzhledem k tomu, že první zaměstnanec používá operační systém Ubuntu a druhý MacOS tak zvýšená úroveň zabezpečení na jejich počítačích není nutností.

5.2.1 Monitoring

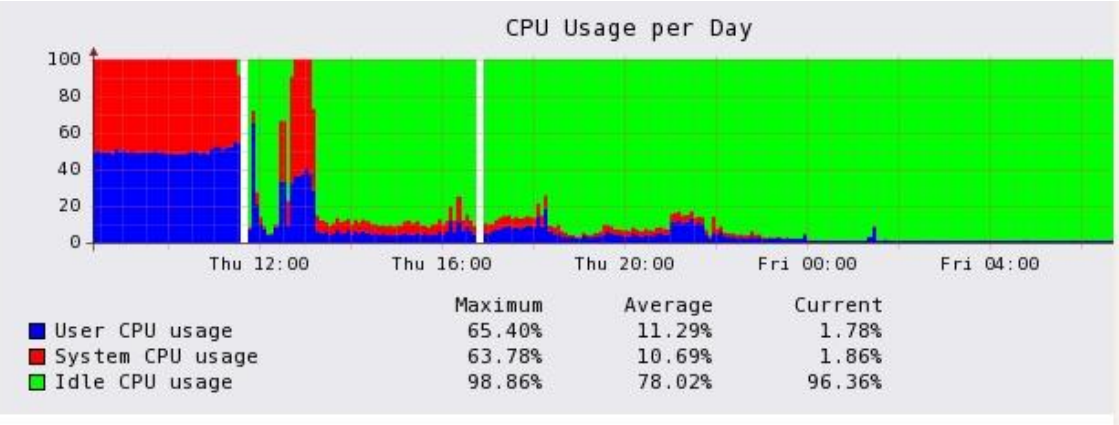
Pro zmapování celé lokální sítě byl použit program The Dude. Schéma lokální sítě ve firmě Crazy Tomato s.r.o. je zobrazeno na následujícím obrázku.



Obrázek 11 - Zobrazení síťové struktury v The Dude

Z obrázku 12 je zřetelná jednoduchá struktura vybrané lokální sítě. Je vidět, že nedochází k žádnému dělení na menší síťové segmenty. V rámci této malé lokální sítě není nutné provádět optimalizaci datových toků a rozmístění prvků.

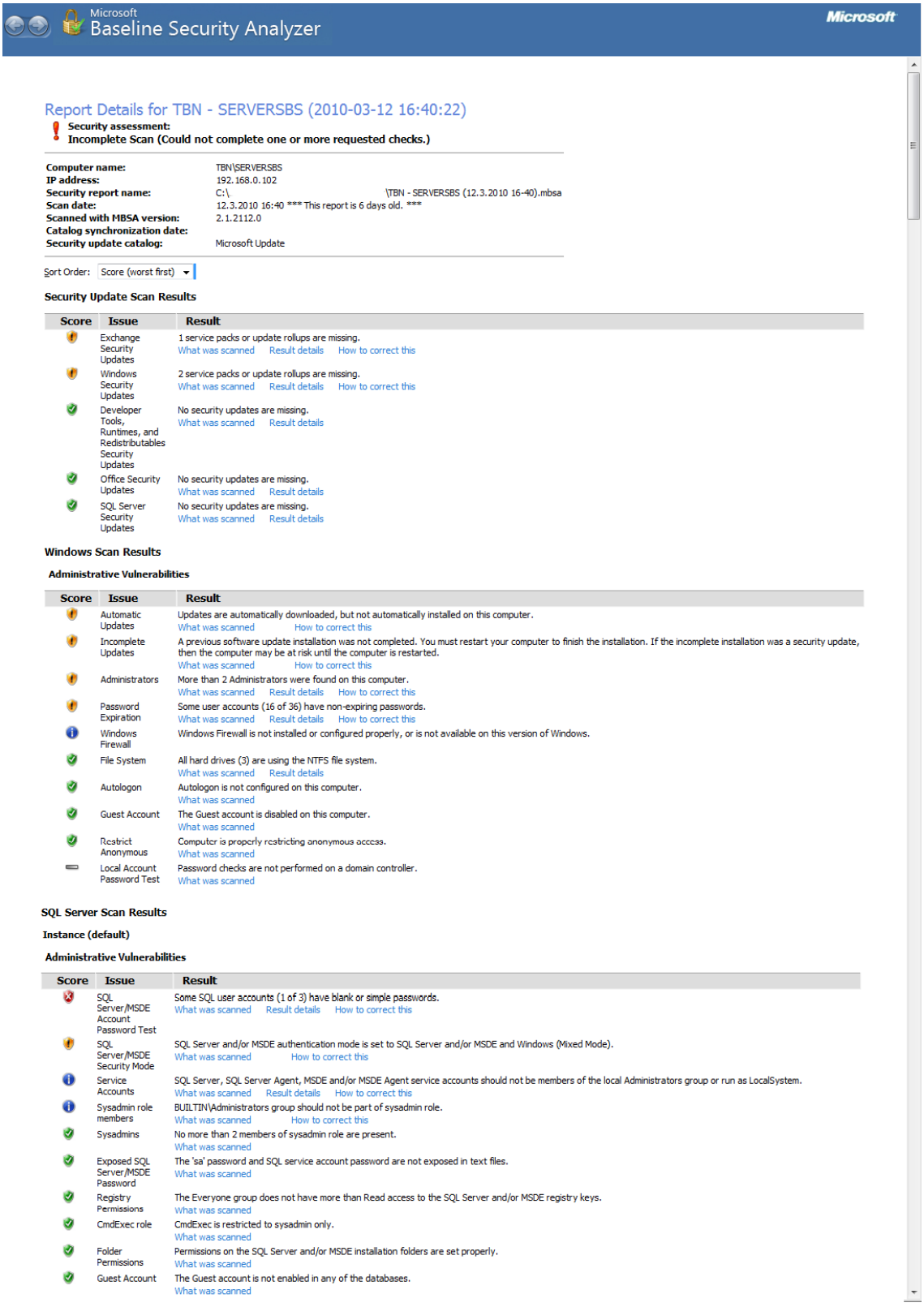
Jako monitorovací nástroj je používán ntop, který je jedním z mnoha modulů, kterými disponuje firewall Endian. Ntop je schopný monitorovat téměř jakýkoliv provozovaný počítač nebo protokol a přehledně zobrazovat jednotlivé části provozu. Jednotlivé statistiky jsou ukládány a je možné je používat pro dlouhodobé analýzy. Ntop zároveň ukládá veškeré vybrané statistiky provozu z ostatních funkcí firewallu a je tedy možné zpětně dohledávat jakékoliv anomálie či problémy. Pokud tedy dojde k narušení bezpečnosti lokální sítě, tak je možné daný problém zpětně dohledat, detailně ho analyzovat a zjistit příčiny nebo odhalit útočníka. Z následujícího obrázku je vidět, že ntop nejen že umí monitorovat síťový provoz, ale zároveň umí sledovat provoz vybraných zařízení a jejich zátěž. Pokud nějaký procesor vykazuje nadprůměrnou zátěž, tak je zřejmé, že jeho výpočetní výkon je zneužíván škodlivým kódem a je třeba zasáhnout.



Obrázek 12 - Ntop a zobrazení zátěže procesoru

Lze konstatovat, že firewall Endian spolu se všemi moduly představuje skvělou alternativu pro programy jako FlowMon či Wireshark.

Pro monitorování a správu uživatelských účtů a hesel je příležitostně používán program MBSA. V rámci bezpečnostní analýzy byl proveden komplexní test celé lokální sítě. Část výsledků je ukázána v následujícím obrázku.



Obrázek 13 - Výsledky MBSA analýzy

Díky tomuto testu byly zjištěny následující problémy:

- Chybějící update u Microsoft Exchange Server – Tento program není využíván a nejedná se tedy o závažnou chybu.
- Dva chybějící updaty pro Microsoft Server 2003
- Updaty nejsou na serveru instalovány automaticky – Některé updaty jsou v prvních verzích někdy nestabilní a jsou tedy instalovány ručně, až po potvrzení jejích stability.
- Přítomnost 2 administrátorských účtů na serveru – Pouze jeden účet je administrátor s plnými právy, druhý účet je používán pouze pro některé specifické služby. Tento fakt tedy nepředstavuje riziko.
- 16 z 36 účtů mají heslo s neomezenou platností – Tento problém byl v minulosti řešen a vzhledem k uživatelskému pohodlí bylo upuštěno od zavedení časové platnosti hesel.
- 1 SQL účet používá prázdné heslo – Po kontrole bylo navíc zjištěno, že daný účet patří pracovnici, která ve firmě nepracuje od roku 2009

Součástí kompletního testu byla i analýza Microsoft##SSEE, SBSMONITORING, SHAREPOINT a desktopových programů. Test vykázal i další menší problémy, které ale nebyly analyzovány vzhledem k jejich malé důležitosti.

Pokud je u jakékoliv položky nalezen problém, tak je automaticky nabídnuto vhodné řešení. V případě chybějících updatů je vytvořen kompletní seznam již nainstalovaných a chybějících. U chybějících updatů je nabídnut odkaz ke stažení, takže administrátor má skutečně možnost jakékoliv problémy řešit ihned a velmi jednoduše.

Díky provedené analýze bylo zjištěno pouze několik závažnějších problémů jako např. SQL uživatelský účet s prázdným heslem, který nikdo již přes rok nepoužívá.

Obdobná analýza proběhla na celé lokální síti, kde bylo zjištěno jen několik závažnějších problémů:

- Zapnutý autologon na 4 počítačích
- Používání slabých hesel na většině počítačů
- Většina hesel má neomezenou platnost
- Objevení různých starých nepoužívaných účtů

Mimo tyto závažnější problémy bylo objeveno množství drobných nedostatků, které ale nepředstavují ani minimální riziko a jejich odstraňováním by byly využity administrátorské hodiny, které by mohly být využity mnohem lépe a efektivnějším způsobem.

5.3 Výhody daného řešení

Bude velice obtížné vybrat nějaká pozitiva u výše analyzované bezpečnostní situace. Jedná se o funkční řešení, které plní svoji funkci správně, ale nikoliv výborně. Celá lokální síť je komplexně zabezpečená na dostatečné úrovni a nelze tedy konstatovat, že by nějaká část či služba byla zabezpečena na maximum svých možností.

1) Firewall Endian poskytuje skvělou úroveň zabezpečení vzhledem k nulové pořizovací ceně. Jedná se komplexní program s celou řadou modulů a různých bezpečnostních prvků jako např. IDS, IPS, Proxy atd. V rámci omezeného rozpočtu je tento firewall skvělá volba. Lze samozřejmě konstatovat, že komerční řešení s pořizovací cenou okolo 20.000Kč bude mít lepší výbavu, podporu či českou lokalizaci, ale pokud je nejdůležitějším faktorem cena tak je Endian Firewall Community edice výbornou volbou a lze to nakonec považovat za pozitivum. V současnosti jsou aktivovány systémy IDS a IPS, které více méně nepotřebují náročnou údržbu. Co se konfigurace IPS týče, tak ta je zvolena tak aby docházelo k minimálnímu počtu falešných pozitiv a nebylo by potřeba častých zásahů ze strany administrátora. IDS i IPS zaznamenávají veškerý nebezpečný i potenciálně nebezpečný provoz (např. skenování portů) a díky záznamům je možné zpětně dohledat jakoukoliv podezřelou aktivitu.

2) Jako antivirový program je používán program ESET NOD, který je provozován jak na pracovních stanicích, tak i na serveru. Jedná se tedy víceúrovňové řešení což lze také hodnotit jako kladný aspekt. V případě detekce jakéhokoliv škodlivého kódu je administrátor upozorněn emailem a může zkontrolovat, zdali došlo ke správnému odstranění hrozby.

3) Jako záložní zdroj energie je používán vhodně dimenzovaný UPS Belkin s kapacitou 1500VA, což v případě problému poskytne všem serverovým prvkům možnost, aby bezpečně uložily veškerá data a samovolně byly vypnuty. Klíčové síťové prvky jsou tedy dobře zabezpečeny proti výkyvům nebo výpadkům v elektrické síti.

4) Wi-Fi síť je zabezpečená na maximum svých možností, přičemž dané omezení je způsobeno zastaralými počítači, které nepodporují novější zabezpečení WPA2. Toto bohužel nelze brát jako omluvu, obzvlášť u Wi-Fi sítě, která představuje jednu z nejrizikovějších oblastí zabezpečení. WPA představuje dobré zabezpečení, ale pro připraveného zkušeného útočníka není prolomení WPA problémem. Na druhou stranu i zabezpečení WPA představuje důležitý prvek, který je v mnohých komerčních Wi-Fi sítích opomíjen. Pro přístup do dané Wi-Fi sítě je navíc používáno silné heslo, takže lze celkové zabezpečení Wi-Fi klasifikovat jako nadprůměrné. Jako možné doplnění pro bezpečnost Wi-Fi lze brát IP či MAC filter, ale po konzultaci s administrátorem bylo shledáno, že tyto 2 služby v samotném výsledku neposkytují znatelný nárust bezpečnosti v porovnání s vynaloženým úsilím. Vysílání SSID je ponecháno aktivní vzhledem k uživatelským žádostem o jednodušší připojovaní k Wi-Fi síti.

5.4 Nevýhody, slabá místa

V této kapitole budou probrána nejzávažnější bezpečnostní rizika. Vybraná lokální síť obsahuje spoustu prvků či služeb, které jsou zabezpečené pouze na dostatečné úrovni, ale jejich stav není přímou hrozbou pro lokální síť. Tyto prvky či služby budou probrány v následující kapitole, kde budou prezentovány spolu s návrhem možných vylepšení.

1) První a zřejmě jednou z nejzásadnějších chyb je umístění serverů a dalších klíčových síťových prvků. Fyzický přístup k těmto prvkům není jakkoliv zabezpečený. Jakákoliv návštěva zanechaná na chvíli bez dozoru či pravidelně docházející paní uklizečka má v podstatě neomezený fyzický přístup k jakékoliv komponentě. Externí disk, na který jsou zálohovány firemní data představuje velmi vážné bezpečnostní

riziko, kdy jakákoliv nepovolaná osoba může tento disk zcizit a získat tím důležitá firemní data, která nejsou ani šifrována. Softwarový přístup k administrátorským funkcím je samozřejmě zabezpečen silnými hesly, ale veškerý fyzický přístup není zabezpečen. Velké riziko představuje i jakákoliv nechtěná nevhodná manipulace. Většina kabelových rozvodů je nechráněna a stačí malé zaškobrtnutí a hlavní server může být za chodu odpojen.

2) Veškeré síťové přípojky nejsou nijak zabezpečeny proti připojení neznámého zařízení. Kdokoliv se tedy může se svým počítačem a síťovým kabelem připojit k lokální síti, začít využívat jejích služeb či hledat bezpečnostní mezery. Tento nedostatek představuje velké potenciální riziko vzhledem k poměrně frekventovaným návštěvám, které chodí do kanceláře firmy.

3) Na pracovních stanicích není spuštěn žádný firewall. Nejedná se o závažný nedostatek, ale protože si zaměstnanci nosí své notebooky i domů, tak by bylo vhodné, aby byly tyto počítače dostatečně zabezpečeny i bez přítomnosti serverového Endian firewallu a dalších bezpečnostních prvků. Druhá vrstva firewallu zároveň zlepší ochranu celé lokální sítě, umožní různé filtrování aplikací a dalších služeb, což není možné provádět prostřednictvím serverové firewall Endian.

4) I přes to, že na lokální síti je zřízena doména, tak ji využívá pouze jeden pracovník. Pro lepší softwarové zabezpečení by bylo jednoznačně vhodnější, kdyby se do domény přihlašovali všichni pracovníci.

5) Na některých počítačích je používán autologon, takže přístup na lokální síť a na lokální pevný disk může mít v podstatě kdokoliv, kdo bude mít k danému počítači přístup. Na jednom z těchto počítačů je dokonce používán účetní program Pohoda, kde se nacházejí důležité informace týkající se firemního účetnictví. Tento počítač by měl být zabezpečen na maximální úroveň.

6) Serverové prvky jsou ve stejném síťovém segmentu jako zbytek pracovních stanic. Jejich softwarová izolace a omezení přístupu by mělo být jednou z priorit.

7) Některé uživatelské účty používají slabá hesla, která jsou navíc časově neomezená, což v kombinaci s používáním normálních uživatelských skupin (oproti doménám) představuje potenciální riziko střední úrovně.

5.5 Možnosti vylepšení bezpečnostní situace

Na základě získaných informací a znalostí z literární rešerše budou v této kapitole navrženy možnosti k vylepšení aspektů, které byly shledány jako rizikové či nedostatečné.

1) Servery a další klíčové síťové prvky – nijak zabezpečený fyzický přístup k těmto prvkům by měl být hlavní prioritou. Vzhledem k tomu, že se typově jedná o běžné počítačové skříně tak jejich stabilní provoz nevyžaduje specifické klimatické podmínky a není nutné nákladně zřizovat speciální místnost. Pro zabezpečení by zcela postačovalo přesunutí do malé uzamykatelné místnosti. Problémem je, že kancelářské prostory žádnou takovouto místností nedisponují. Servery jsou umístěny v místě, kde jsou umístěny hlavní rozvaděče a kabeláž, což by zcela jistě znesnadnilo jakýkoliv přesun. Uzamykání celé místnosti také není možné, protože v dané místnosti běžně pracují 1 až 3 zaměstnanci. Jediným vhodným řešením tohoto problému je pořízení vhodně dimenzované serverové skříně, do které by byly všechny tyto klíčové síťové prvky umístěny. Toto řešení by zároveň odstranilo riziko vytržení nějakého důležitého kabelu, protože většina kabeláže by byla umístěna v dané serverové skříni. Bylo by nejvhodnější do dané skříně umístit i monitor a ovládací periferie, ale to už by vyžadovalo zbytečně velkou skříň, která je dražší. Vhodnou volbou by tedy bylo umístění pouze serveru, UPS a záložního disku do serverové skříně a ponechání monitoru a ovládacích periferií na stole poblíž. Důležité prvky by tedy byly uzamčeny a chráněny jako proti neopatrnosti pracovníků tak proti rizikům jako je krádež apod.
Pořizovací cena by měla být max 5.000Kč.

2) Servery by měly být také oddělené na softwarové úrovni, což by bylo možné provést zavedením demilitarizované zóny. Investicí by v tomto případě bylo pořízení nového serveru, který by umožňoval provoz a správu vytvořené DMZ. Tímto způsobem

by byly veškeré klíčové služby zabezpečeny na vyšší úrovni. Přístup k těmto službám by byl omezený v obou směrech a byla by eliminována většina potenciálních rizik. Pořizovací cena by se pohybovala okolo 5.000 Kč.

3) Zabezpečení síťových portů patří také mezi jednu z priorit. Nejlepším řešením je bezesporu využití protokolu 802.1X. Nevýhodou tohoto protokolu je nutnost pořízení speciálních switchů, které se pohybují v cenovém rozmezí od 8.000Kč a výše. Jedním z nejlevnějších produktů je např. 3COM Baseline Switch 2250 Plus, který stojí 8.299Kč. Problém je, že většina malých a středních firem nenajde upotřebení pro takovýto druh switche a jedná se tedy pouze o investici pro 802.1X.

4) Úroveň zabezpečení uživatelských účtů je podprůměrná a mělo by být prioritou, aby pracovníci akceptovali nové bezpečnostní postupy, které by měly být zavedeny. Jedním ze základních pilířů uživatelské bezpečnosti by mělo být zavedení Active Directory domény pro všechny uživatele. Pro danou doménu by měla být také nastavena alespoň minimální bezpečnostní politika, která by omezila počet nepodařených přihlášení atd. Součástí celé této změny by mělo být také povinné zavedení bezpečných hesel, které by splňovaly minimálně body 1,5 a 6. Deaktivace funkcí jako autologon by měla být samozřejmostí.

5) Zaměstnanci, kteří využívají Wi-Fi pro připojení k lokální síti by měli být instruováni, aby spíše preferovali kabelové připojení. Pokud daný zaměstnanec pracuje pouze na jednom pracovním místě, tak není důvod, aby používal Wi-Fi. Kabel nejen že poskytuje garantovanou rychlost připojení, ale je také mnohem bezpečnější. Jak bylo ukázáno, tak zabezpečení Wi-Fi představuje téměř nemožný úkol. Ve vybrané firmě je zabezpečení Wi-Fi nadprůměrné, ale rozhodně nikoliv na optimální úrovni a proto by měl každý zaměstnanec zkusit obětovat malý kus pohodlí a připojovat se přes kabel. Při přesunu do zasedací místnosti není problémem přepnout na krátkou dobu na Wi-Fi a zase obráceně.

6) Používaný firewall Endian disponuje také funkcí Proxy, která umí zabezpečit protokoly jako SMTP, HTTP a FTP. V rámci SMTP Proxy je možné např. aktivovat

anti-spamový filtr či antivirový program. Tyto služby se starají o zabezpečení poštovních zpráv automaticky a mimo dosah zaměstnaneckých počítačů. V rámci HTTP Proxy je možné např. velmi efektivně filtrovat veškerý obsah stránek, které si zaměstnanci prohlížejí. Nejedná se jen o způsob kontroly, ale zároveň zabezpečení proti nezkušeným uživatelům. Aktivace Proxy pro jakýkoliv protokol vyžaduje konfiguraci a zároveň pravidelnou administrátorskou údržbu.

7) Wi-Fi síť je zabezpečena protokoly WEP a WPA, což bylo shledáno jako nadprůměrné, ale nikoliv optimální. Protokol WPA2 bohužel není podporován dvěma zastaralými notebooky. V rámci jednoho či dvou let by bylo vhodné nahradit tyto notebooky za novější, které budou podporovat tyto funkce a ihned aktivovat protokol WPA2 pro Wi-Fi síť. V rámci zvýšení bezpečnosti Wi-Fi by bylo dodatečně možné zavést protokol 802.1X, který je podporován velkým množstvím dnešních routerů a v rámci možného upgradu routerů by bylo určitě vhodné zvážit toto kritérium. Dodatečným zabezpečením by bylo zavedení protokolu VPN pro veškeré Wi-Fi přenosy, což by mnohonásobně zvýšilo bezpečnost přenášených dat, jelikož by byly automaticky šifrované. Na jedné straně by tedy bylo vhodné zabezpečit samotnou Wi-Fi síť pomocí WPA2 či 802.1X a zároveň zabezpečit přenášená data šifrováním přes VPN.

8) Na uživatelské počítače by měl být instalován firewall. Toto by vytvořilo víceúrovňovou architekturu a samotné pracovní stanice by byly lépe zabezpečeny. Prostřednictvím těchto lokálních firewallů by bylo možné nastavovat různé aplikační filtry a obecně tak zlepšit ochranu lokální sítě proti neznalému či neopatrnému pracovníkovi. Lze samozřejmě vybírat z komerčních a open source produktů a v případě nedostatku financí zvolit volně šiřitelnou variantu, která poskytne alespoň částečné zlepšení.

5.5.1 Ekonomická analýza možných vylepšení

Tato kapitola by měla analyzovat důležitost jednotlivých návrhů z předchozí kapitoly a výsledkem by měl být konečný návrh, který by zohledňoval jak finanční tak i bezpečnostní kritéria.

Pokud všechna doporučení seřadíme dle jejich důležitosti vzhledem k bezpečnosti, tak dostaneme následující seznam (seřazeno od nejdůležitějšího):

1) Fyzické zabezpečení klíčových síťových prvků
2) Uživatelské účty
3) Síťové porty a 802.1X
4) DMZ – softwarové zabezpečení serverů
5) Instalace firewallu na pracovní stanice
6) Wi-Fi síť – VPN, nové notebooky a přechod na WPA2
7) Aktivace Proxy v Endian firewallu
8) Používání kabelu před Wi-Fi

První tři body představují velká bezpečnostní rizika, která by měla být řešena co nejdříve. První bod lze klasifikovat jako kritický. Bezproblémový chod serverů a dalších klíčových prvků je pro provoz firmy zcela zásadní a bez přístupu k poště a internetu nemůže většina zaměstnanců jakkoliv vykonávat svou práci. Tyto síťové prvky nejsou také zabezpečeny proti krádeži a firma může přijít např. o externí disk, na kterém jsou uložena důležitá data. Ztráta takovýchto dat může pro firmu znamenat celkem zásadní problém, kdy lze přijít o důvěru obchodních partnerů, snížení konkurenceschopnosti atd.

Pokud bychom doporučení seřadili dle jejich pořizovací ceny (včetně práce IT externisty) tak dostaneme následující seznam (seřazeno od nejmenší ceny):

1) Používání kabelu před Wi-Fi – cena 0 Kč
2) Uživatelské účty – cena do 500 Kč
3) Instalace firewallu na pracovní stanice – cena do 1.000 Kč
4) Aktivace Proxy v Endian firewallu – cena do 500 Kč + pravidelná údržba
5) Fyzické zabezpečení klíčových síťových prvků – cena okolo 5.000 Kč
6) DMZ – cena okolo 5.000 Kč

7) Síťové porty a 802.1X – od 8.000 Kč

8) Wi-Fi síť – cena od 10.000 Kč

Pokud porovnáme obě tabulky, tak lze vyvodit určité celkové doporučení. Firma Crazy Tomato s.r.o. má pro rok 2010 rozpočet pro rozvoj informačních a komunikačních technologií 15.000 Kč. Bylo naplánováno, že tato částka bude použita k pořízení nového notebooku namísto zastaralé pracovní stanice. Po provedení bezpečnostní analýzy by měla být tato investice odložena a vyhrazené finance by měly být investovány do zlepšení zabezpečení. Pokud tedy vybereme doporučení, které bylo shledáno jako důležité a zároveň představuje přijatelnou investici, tak se jednoznačně jedná o bod 2, čímž je kompletní re-konfigurace uživatelských účtů. S ohledem na zmíněný rozpočet lze na druhé celkové místo zařadit fyzické zabezpečení klíčových síťových prvků. Tyto 2 doporučení by měly bezesporu být první v pořadí a jejich provedení by mělo být prioritou. Třetím nejdůležitějším (z hlediska bezpečnosti) doporučením je zabezpečení síťových portů. Toto doporučení by bylo realizovatelné v rámci rozpočtu, ale poté by nezbyly téměř žádné finance na další doporučení. Lze navrhnout, aby tato investice byla zařazena do rozpočtového plánu pro příští rok. Jako vhodnější investice se jeví zřízení DMZ, což nebylo shledáno natolik závažným problémem, ale pořizovací cena natolik nezatíží rozpočet. Dalšími vhodnými investicemi jsou bod 3 (firewall na pracovní stanice) a 4 (Proxy v Endian firewallu). Bod 1 je pouhým návrhem a nevyžaduje jakékoliv investice a závisí pouze na daném administrátorovi, jak se dohodne s uživateli. Lepší zabezpečení Wi-Fi sítě by bylo možné pouze s větším rozpočtem, kdy by se daly pořídit nové notebooky, které by umožnily provoz WPA2 protokolu. Možnou alternativou může být používání VPN protokolu pro komunikaci ve Wi-Fi, což by alespoň částečně snížilo potenciální riziko.

Pokud tedy vezmeme v úvahu aktuální rozpočet a rozumné časové rozložení investic, tak by jako první měla být provedena kompletní re-konfigurace uživatelských účtů. Následovat by mělo fyzické zabezpečení serverů. Zřízení DMZ by mělo následovat jako třetí, ale v případě dočasně omezených prostředků by bylo vhodnější tuto investici o několik měsíců odložit a místo ní zvolit další body jako např. instalace firewallů na pracovní stanice.

6 Závěr

Tématem této práce byl návrh optimálního zabezpečení a monitoringu lokální sítě v malé až střední firmě. Na základě poznatků získaných v literární rešerši byla vytvořena optimální konfigurace, která obsahovala výčet různých postupů či programů.

Literární rešerše i optimální konfigurace byly rozděleny do 4 kapitol – hardwarové a softwarové zabezpečení, Wi-Fi a monitoring. Z hlediska hardwarového zabezpečení je klíčové umístění důležitých síťových prvků jako např. servery. Tyto prvky musí být chráněny proti všem možným vlivům jako výpadek elektrického proudu apod. Pro stabilizaci a záložní dodávku elektrického proudu je vhodné použít záložní zdroj. Zabezpečení všech síťových portů je vhodné realizovat přes protokol 802.1X.

U softwarového zabezpečení byla pouze okrajově zmíněna vhodnost operačních systémů pro různé úrovně uživatelů, přičemž operační systémy na bázi Linux jsou vhodné pouze pro pokročilé uživatele. Uživatelské skupiny (bez ohledu na operační systém) by měly fungovat nejlépe pod systémem Active Directory a měly by podléhat přísným omezením vztahujícím se k pracovním náplním jednotlivých zaměstnanců. Důležitá hesla by měla splňovat všechny podmínky pro silná hesla. Na každé pracovní stanici by měl být nainstalován antivirový program a firewall, aby byla vytvořena (nejlépe heterogenní) víceúrovňová architektura. Pro pokročilou úroveň zabezpečení je nutné používat systém IDS/IPS či IDPS a zároveň mít serverové služby v oddělené demilitarizované zóně. Pomocí více-kriteriální analýzy byly porovnány hardwarové a softwarové produkty, které nabízejí podobné služby, a bylo zjištěno, že hardwarové produkty s integrovanými bezpečnostními prvky nabízejí funkce pro komplexní zabezpečení a navíc za nižší cenu oproti softwarovým řešením. Zabezpečení Wi-Fi sítě by mělo být realizováno nejlépe přes protokoly WEP, WPA a WPA2. Každý uživatel by se měl k Wi-Fi připojovat přes VPN aby veškerá přenášená data byla šifrována.

V kapitole monitoringu byly přímo porovnávány komerční programy s volně šiřitelnými. Bylo zjištěno, že kombinací dvou volně šiřitelných programů lze téměř nahradit komerční řešení. Kombinací programů Wireshark a Dude lze získat účinný nástroj pro detailní monitorování veškerého síťového provozu a zároveň je možné vytvářet grafická schémata, ukládat statistiky a tedy celkově dlouhodobě optimalizovat lokální síť. Nevýhodou je absence české lokalizace a podpora ze strany dodavatele.

Hlavním cílem této práce bylo použití výše zmíněné optimální konfigurace k provedení bezpečnostní analýzy ve vybrané firmě. Na základě výsledků byly vyzdvihnuty silné stránky vybrané lokální sítě, ale hlavním cílem tohoto bezpečnostního auditu bylo nalezení slabých míst, která by představovala potenciální riziko pro ohrožení bezpečnosti. Bezpečnostním rizikem bylo shledáno hardwarové i softwarové zabezpečení klíčových síťových prvků, nechráněné síťové porty, velmi špatně zabezpečené uživatelské účty, absence firewallu na pracovních stanicích a nedostatečně zabezpečená Wi-Fi. Na základě optimální konfigurace byl vytvořen seznam doporučení včetně orientačních cen. Doporučení byla seřazena dle priority a ceny a následně byl vytvořen konečný seznam, který zohledňoval obě kritéria. Na základě omezeného ročního rozpočtu bylo nutné upravit seznam doporučení a bohužel bylo zjištěno, že není možné realizovat všechna doporučení v rámci jednoho roku. Seznam byl tedy přepracován a rozvržen, tak aby během prvního roku byla realizována 2 nejdůležitější doporučení spolu s většinou méně důležitých. Tímto způsobem budou odstraněna téměř všechna rizika v nejkratším možném čase a v průběhu následujícího roku bude možné odstranit všechna zbývající rizika.

Bylo prokázáno, že rozpočet malé firmy představuje reálný omezující faktor a ani v případě objevení závažných bezpečnostních nedostatků není možné realizovat nápravu všech problémů. S omezeným rozpočtem je opravdu obtížné vytvořit komplexní zabezpečení na dostatečné úrovni. Jednou možností je úspora na určitých segmentech a pořízení pouze několika profesionálních řešení. Tento způsob je jednostranně dimenzovaný a lokální síť poté obsahuje spoustu bezpečnostních mezer. Druhý způsob zabezpečení byl demonstrován v této práci a jeho hlavním atributem je komplexní zabezpečení lokální sítě na alespoň minimální úrovni. Bylo prokázáno, že lze nalézt volně šiřitelné programy, které poskytnou dostatečné zabezpečení a přitom jsou zdarma. Takto ušetřené finance lze investovat do takových produktů, které nelze nahradit jakýmkoliv levným nebo volně šiřitelným řešením. Ve vybrané firmě bylo ukázáno, že použití volně šiřitelného firewallu ušetřilo finance, které byly následně investovány do záložního zdroje a záložního disku. Tyto dva prvky patří mezi nepostradatelné v síťové infrastruktuře, a pokud by byly vynechány z důvodu nedostatku financí, tak by provedená bezpečnostní analýza dopadla podstatně hůře.

7 Seznam použitých zdrojů

1) HORÁK, Jaroslav. Bezpečnost malých počítačových sítí. 1. vydání. Praha: Grada, 2003. 200 s. ISBN 80-247-0663-6

2) BITTO, Ondřej. Jak zabezpečit domácí a malou síť Windows XP. 1. vydání. Brno: Computer Press, 2006. 216 s. ISBN 80-251-1098-2

3) DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. 1. vydání. Brno: Computer Press, 2004. 200 s. ISBN 80-251-0106-1

4) *OSI Model – SAMURAJ-cz.com* [online]. c2007, poslední revize 05.03.2007 [cit. 2010-02-03]. Dostupné z <http://www.samuraj-cz.com/clanek/osi-model/>.

5) *Síťový model TCP/IP* [online]. c2006 [cit. 2010-02-03]. Dostupné z <http://pc-site.owebu.cz/?page=PTCPIP>.

6) *TCP/IP – Wikipedie, otevřená encyklopedie* [online]. c2007, poslední revize 5.02.2009 [cit. 2010-02-21]. Dostupné z < http://cs.wikipedia.org/wiki/TCP/IP >.

7) *Active Directory – Wikipedie, otevřená encyklopedie* [online]. c2005, poslední revize 16.09.2009 [cit. 2010-02-20]. Dostupné z <http://cs.wikipedia.org/wiki/Active_Directory>.

8) *Systémy pro detekci neoprávněného průniku – Časopis IT Systems – 7-8 2003* [online]. c2003, poslední revize 07.2003 [cit. 2010-01-02]. Dostupné z <http://www.systemonline.cz/clanky/systemy-pro-detekci-neopravneneho-pruniku.htm>.

9) *Systémy prevence průniků (1) – jen detekovat nestačí* [online]. c2007, poslední revize 5.11.2007 [cit. 2010-01-03]. Dostupné z <http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&clanekID=331>.

10) *Wi-Fi - Wikipedie, otevřená encyklopedie* [online]. c2004, poslední revize 11.12.2009 [cit. 2010-02-10]. Dostupné z <http://cs.wikipedia.org/wiki/Wi-Fi>.

12) *Wired Equivalent Privacy - Wikipedie, otevřená encyklopedie* [online]. c2006, poslední revize 18.1.2010 [cit. 2010-02-10]. Dostupné z <http://cs.wikipedia.org/wiki/Wired_Equivalent_Privacy>.

13) *Wi-Fi Protected Access - Wikipedie, otevřená encyklopedie* [online]. c2006, poslední revize 16.2.2009 [cit. 2010-02-18]. Dostupné z <http://cs.wikipedia.org/wiki/Wi-Fi_Protected_Access>.

14) *Virtuální privátní síť - Wikipedie, otevřená encyklopedie* [online]. c2006, poslední revize 1.11.2009 [cit. 2010-02-19]. Dostupné z <http://cs.wikipedia.org/wiki/Virtu%C3%A1ln%C3%AD_priv%C3%A1tn%C3%AD_s%C3%AD%C5%A5>.

15) VPN (2) – Internet versus plně privátní sítě [online]. c2003, poslední revize 8.1.2003 [cit. 2010-02-17]. Dostupné z <http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&clanekID=221>.

16) Wi-Fi – (bezdrátový internet) – úvod, zabezpečení, struktura [online]. c2007, poslední revize 26.12.2007 [cit. 2010-02-11]. Dostupné z <http://mb.optimax.cz/2007/12/26/wirelless/Wi-Fi-bezdratovy-internet-uvod-zabezpeceni-struktura>.

17) *Jak na ochranu a zabezpečení Wi-Fi sítí | HW.cz* [online]. c2003, poslední revize 3.7.2003 [cit. 2010-02-11]. Dostupné z < http://hw.cz/ethernet/Wi-Fi/Wi-Fi_ochrana.html>.

18) *Netflow - Wikipedie, otevřená encyklopedie* [online]. c2008, poslední revize 26.3.2009 [cit. 2010-01-16]. Dostupné z <http://cs.wikipedia.org/wiki/Netflow>.

19) *Wireshark - Wikipedie, otevřená encyklopedie* [online]. c2006, poslední revize 21.9.2009 [cit. 2010-01-21]. Dostupné z <http://cs.wikipedia.org/wiki/Wireshark>.

20) *SNMP – Simple Network Management Protocol - SAMURAJ-cz.com* [online]. c2006, poslední revize 20.12.2006 [cit. 2010-02-07]. Dostupné z <http://www.samuraj-cz.com/clanek/snmp-simple-network-management-protocol/>.

8 Přílohy