Česká zemědělská univerzita v Praze
Provozně ekonomická fakulta
Katedra informačních technologií

Zabezpečení Wi-Fi sítí

Bakalářská práce

Autor: **Ivo Gec**
Vedoucí práce: Ing. Pavel Šimek, Ph.D.

2016

Prohlášení

Prohlašuji, že jsem bakalářskou práci na téma: **Zabezpečení Wi-Fi sítí** vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů.

Jsem si vědom, že odevzdáním bakalářské práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby.

Jsem si vědom, že moje bakalářská práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí.

Jsem si vědom že, na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.

Ivo Gec

V Praze dne 13. 3. 2016

Poděkování

Rád bych poděkoval panu Ing. Pavlu Šimkovi, Ph.D. za vedení mé bakalářské práce a za jeho cenné připomínky a rady v rámci bakalářského semináře. A také bych rád dal velké díky mé přítelkyni za pevné nervy semnou při tvorbě bakalářské práce.

Souhrn

Bakalářská práce je tematicky zaměřena na bezpečnost bezdrátových sítí pracujících na frekvenčních pásmech 2,4 GHz a 5 GHz. Teoretická část bakalářské práce je věnována problematice bezdrátové technologie. V teoretické části bakalářské práce jsou obsaženy jednotlivé standardy, režimy provozu, možné útoky, mechanismy a zabezpečení, která případným útokům, nebo hrozbám předchází. Praktická část bakalářské práce popisuje možný návrh zabezpečení pro firmu, jež se zabývá účetnictvím a daněmi.

Summary

Bachelor thesis is thematically focused on the security of wireless networks operating on frequency bands of 2.4 GHz and 5 GHz. The theoretical part of bachelor thesis is devoted to problemacy of wireless technology. In teoretical part of bachelor thesis are contained various standards, modes of operations, possible attacks, mechanisms and security, which prevent probably attacks or threats. Practical part of bachelor thesis describes a possible design of security for this company, which deals with accounting and taxes.

Klíčová slova

Wi-Fi, zabezpečení, WPA, WEP, WPA2, WEP plus, MAC Access List, VPN, standard IEEE 802.11, Man in the Middle, DDoS.

Key Words

Wi-Fi, security, WPA, WEP, WPA2, WEP plus, MAC Access List, VPN, standard IEEE 802.11, Man in the Middle, DDoS.

Obsah

1 Úvod 9
2 Cíl a metodika práce 10
3 Teoretická východiska 11
3.1 Bezdrátové sítě 11
3.1.1 Rozdělení bezdrátových sítí 11
3.2 Wi-Fi 13
3.2.1 Historie 14
3.3 IEEE 802.11 15
3.3.1 IEEE 802.11a 16
3.3.2 IEEE 802.11b 16
3.3.3 IEEE 802.11g 16
3.3.4 IEEE 802.11n 16
3.4 Režimy provozu 16
3.4.1 Režim infrastruktury 17
3.4.2 Režim Ad-hoc 17
3.5 Výhody a nevýhody 18
3.6 Útoky a hrozby 18
3.6.1 Odposlech 19
3.6.2 DoS 19
3.6.3 Man in the Middle 20
3.6.4 Útok hrubou silou 20
3.7 Bezpečnost sítě 21
3.7.1 Bezpečnostní služby v sítích 21
3.7.2 Šifrování 22
3.8 Zabezpečení Wi-Fi sítě 24
3.8.1 Skrytí SSID 24
3.8.2 WEP 24

3.8.3 WEP2 25
3.8.4 WPA 25
3.8.5 802.11i 26
3.8.6 Filtrace MAC adres 27
3.8.7 VPN 28
4 Vlastní řešení 30
4.1 LAN 30
4.2 Wi-Fi 31
4.2.1 Nastavení bezdrátové sítě 31
4.2.2 Nastavení Firewallu 31
4.3 WAN 32
4.4 Možná řešení zabezpečení 32
4.4.1 Zabezpečení pomocí MAC adres 32
4.4.2 Zabezpečení pomocí VPN 33
4.4.3 Zabezpečení pomocí RADIUS serveru 35
4.5 Zhodnocení VPN poskytovatelů 37
4.6 Doporučení vhodného řešení pro fiktivní společnost 39
5 Zhodnocení výsledků 42
6 Závěr 44
7 Použitá literatura a zdroje 45

Seznam Obrázků

Obrázek 1 WPAN včetně Bluetooth 11
Obrázek 2 WLAN 12
Obrázek 3 WMAN 13
Obrázek 4 WWAN 13
Obrázek 5 Wi-Fi Certified 14
Obrázek 6 Režim infrastruktury 17
Obrázek 7 Režim Ad-hoc 18
Obrázek 8 Schéma DDoS 19
Obrázek 9 Man in the Middle 20
Obrázek 10 Symetrické šifrování 23
Obrázek 11 Asymetrické šifrování 23
Obrázek 12 CMD 27
Obrázek 13 Omezení přístupu 28
Obrázek 14 Rozvod kabeláže 31
Obrázek 15 RADIUS server 36

Seznam Tabulek

Tabulka 1 Přehled standardů IEEE 802.11 15
Tabulka 2 VPN poskytovatelé 37
Tabulka 3 Preferenční tabulka 39

1 Úvod

S masivním rozvojem výpočetní techniky a její cenovou dostupností se již dnes ve spoustě domácností nevyskytuje pouze jeden „pevný“ počítač a telefonní linka. Dnes je domácnost vybavena spoustou „mobilních“ zařízení, která pracují s Wi-Fi připojením pro přístup na internet, bohužel, s tímto moderním trendem bylo třeba navýšit ochranná opatření jednotlivých zařízení v domácnosti, či firmě, která přistupují na internet skrze bezdrátové sítě.

Dnešní bezdrátové sítě jsou významnou součásti datové sítě obecně. Přenosová rychlost se zatím nemůže plně vyrovnat kabelovému připojení. Přednostmi bezdrátové sítě jsou nižší pořizovací cena a možnost dálkového přenosu dat, avšak pouze do vzdálenosti, kde je ještě zařízení schopno přijímat signál od vysílače, který poskytuje bezdrátovou technologii a možnost použití bezdrátové technologie v místech, kde by instalace pevného připojení byla příliš nákladná.

Na rozdíl od pevného připojení k internetu zde vznikl velký problém s ochranou dat při přenosu z jednotlivých zařízení, je to tím, že data, která jsou přenášena vzduchem pomocí elektromagnetického vlnění je možno v dosahu sítě odposlechnout, či jinak zneužít. Wi-Fi sítě se staly nejčastějším místem útoků na domácí, nebo firemní sítě, protože útočník hledá a snaží se dostat do vnitřní sítě přes bezpečností trhliny, které mohou nastat při chybném nastavení Wi-Fi routeru, či podcenění bezpečnostních politik firmy.

Situace jsou si útočnicí plně vědomi a snaží se ji využít ve svůj prospěch na úkor napadené osoby (firmy) za účelem poškození dobrého jména, nebo vydírání. Softwaroví, nebo hardwaroví vývojáři řešení jsou si též plně vědomi dané situace a snaží se navrhnout optimální řešení pro úplnou nebo minimální možnost napadení vnitřní sítě.

2 Cíl a metodika práce

Bakalářská práce je zaměřena na bezpečnost bezdrátových sítí. Hlavním cílem bakalářské práce je navržení optimálního zabezpečení podnikové Wi-Fi sítě, která zahrne bezpečnostní řešení do podnikové infrastruktury.

Mezi ostatní cíle bakalářské práce patří: vypracování přehledů o vývoji bezdrátových sítí, vybraných útoků a jednotlivých metod zabezpečení, jež slouží pro ochranu Wi-Fi sítě.

Metodika práce byla založena na sběru a postupné analýze odborné literatury, a odborných článků v rámci Internetu. Teoretická část popisuje rozdělení bezdrátových sítí, subjektivně vybrané protokoly Wi-Fi, provozy bezdrátové sítě, možné útoky na bezdrátové sítě, včetně jejich zabezpečení proti těmto útokům. Praktická část bakalářské práce je zpracována z osobních zkušeností správy sítě, která je obohacena o nabyté osobní zkušenosti z dodavatelské společnosti.

3 Teoretická východiska

Teoretická část bakalářské práce popisuje rozdělení bezdrátových sítí, historický vývoj Wi-Fi sítí, jednotlivé standardy, režimy provozu, možné útoky a hrozby, jež jsou často na bezdrátové sítě vedeny a jejich následné protiklady v podobě zabezpečení, která mají za úkol možné útoky, či hrozby omezit, nebo úplně eliminovat.

3.1 Bezdrátové sítě

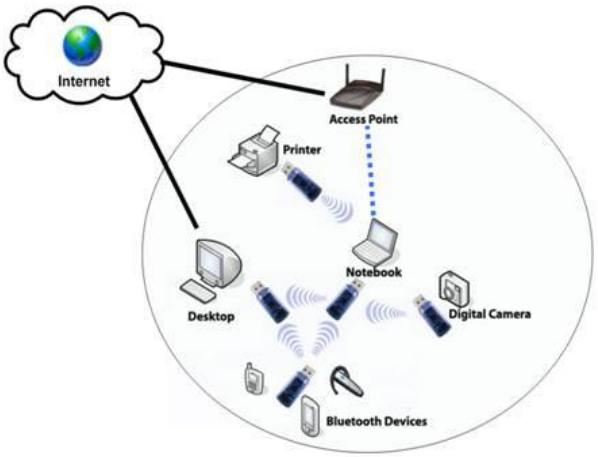
Bezdrátové sítě jsou sítě umožňující přenášet data na krátké, nebo dlouhé vzdálenosti, bez nutnosti využití „pevného“ připojení pro přístup na Internet v oblasti, kde by byla výstavba „pevného“ připojení velmi nákladná. V dnešní době jsou bezdrátové sítě nejčastěji využívány přenosnými zařízeními.

3.1.1 Rozdělení bezdrátových sítí

Rozdělení bezdrátových sítí je závislé na délce vysílaného signálu od přístupového bodu k zařízení, které je schopno vyslaný signál přijmout.

Základní rozdělení bezdrátových sítí je následné:

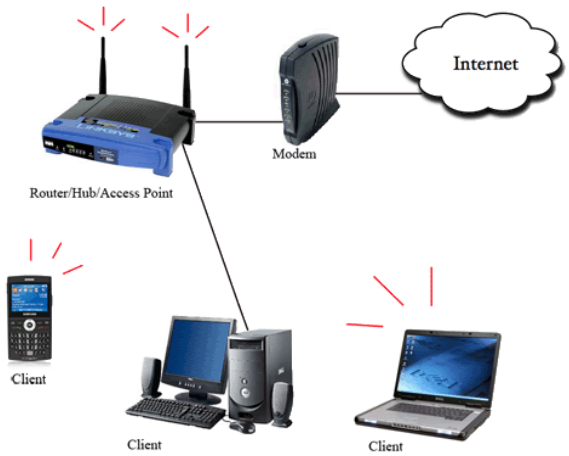
- **Bezdrátová osobní síť WPAN (Wireless Personal Area Network) —** WPAN je síť velmi krátkého dosahu (přibližně deset metrů). [7] Síť sice umožní uživateli bezdrátové připojení k Internetu, avšak, spojení může být využito pouze v rámci jedné místnosti. WPAN slouží především k propojení zařízení např. myši, klávesnice, mobilního telefonu, tiskárny, kde zařízení mezi sebou komunikuji v režimu Ad-hoc, což znamená, že spolu přímo komunikují.



Obrázek 1 WPAN včetně Bluetooth, zdroj: http://www.spiritdatacapture.co.uk/wpan.asp

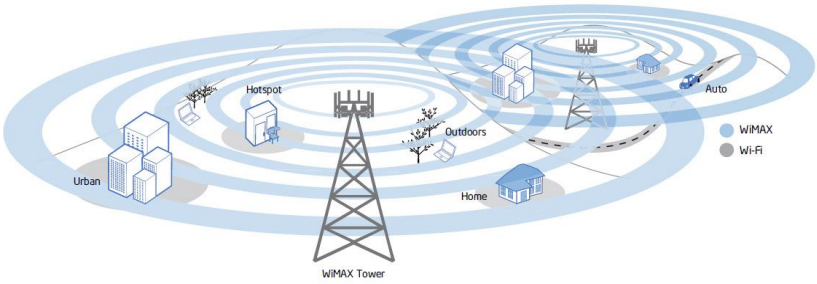
- **Bezdrátové místní sítě WLAN (Wireless Local Area Network) —** Představitelem WLAN sítě je standard Wi-Fi [7], který je normalizován institucí IEEE ve skupině 802.11, standard IEEE 802.11 bude podrobně v následné kapitole rozebrán. Hlavním účelem standardu Wi-Fi je náhrada „drátové“ sítě se snahou o co největší mobilitu a současně o odstranění obtížně instalované síťové kabeláže. S touto situací začaly vznikat v restauracích, na letištích, či v hotelech tzv. „hot spoty“ (přístupové body), které umožňují uživatelům přistupovat na Internet. Situace využili poskytovatelé Internetu (ISP — Internet Service Provider), jenž začali poskytovat koncovým zákazníkům Internet pomocí Wi-Fi sítě, avšak to s sebou může nést i jisté problémy v podobě častého výpadku sítě, nebo rušení signálu přijímaného z vysílače.

Data v rámci sítě WLAN jsou přenášena pomocí směrovače (router), aktivní síťové zařízení umožňuje ostatním zařízením připojení na Internet. Dosah signálu u WLAN závisí na okolních překážkách (budovy, počasí, aj.), které musí signál z vysílače překonat k připojenému zařízení. [8]



Obrázek 2 WLAN, zdroj: http://nokiacompany.tumblr.com/post/8474166208/wlan

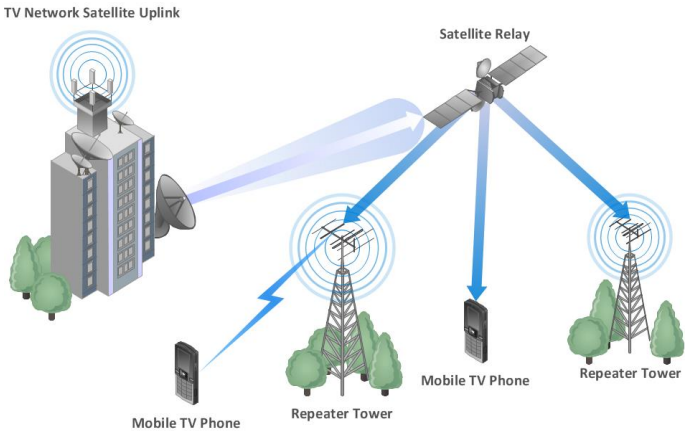
- **Bezdrátové metropolitní sítě WMAN (Wireless Metropolitan Area Network) —** Síť WMAN je navržena pro bezdrátový přenos v rámci (např. sídliště, vesnice, aj.). Jejím největším zástupcem je Wi-Max, který je institucí IEEE normalizován ve skupině 802.16, která má možnost přenosu dat bez přímé viditelnosti (NLOS — Non Line of Sight). [7]



Obrázek 3 WMAN, zdroj: http://escreveassim.com.br/2012/04/17/redes-lan-man-wan-pan-san-can-wman-wwan-e-ran-qual-a-diferenca/

- **Bezdrátové rozsáhlé sítě WWAN (Wireless Wide Area Network) —** Jedná se o síť mobilního širokopásmového připojení, která je v současné době využívána pouze infrastrukturou mobilních operátorů. Z Výše uvedených příkladů má největší pokrytí, jelikož mohou poskytovat konektivitu všude, kde je k dispozici mobilní služba poskytovatele. [7]

V České Republice jsou v současné době využívány mobilní sítě GSM (s technologiemi GPRS a EDGE), UMTS (s technologiemi HSDPA a HSUPA), CDMA2000 (s technologiemi CDMA2000 1xEV-DO a CDMA2000 1xRTT) a od roku 2012 mobilní síť LTE. [9]



Obrázek 4 WWAN, zdroj: http://www.conceptdraw.com/How-To-Guide/wireless-network-wan

3.2 Wi-Fi

Wi-Fi (Wireless Fidelity) sítě pracují na bezdrátové technologii, která je založena na mikrovlnném spojení. Wi-Fi využívá tzv. bezlicenčního pásma, to znamená, že bezdrátové sítě Wi-Fi jsou vhodné pro tvorbu výkonné sítě, kde není potřeba, nebo není možnost vybudovat drátovou síť.

Obrázek 5 Wi-Fi Certified, zdroj: http://myimagecollection.net/wifi+logo+white

3.2.1 Historie

Historie Wi-Fi sítí začala v červnu roku 1997, kdy byl oficiálně vydán první standard IEEE 802.11 vytvořen společností IEEE (Institute of Electrical and Electronics Engineers), standard dosahoval maximální přenosové rychlosti 2 Mbit/s, ani samostatný dosah nebyl nijak daleký. Přenos dat využíval modulaci FHSS (Frequency Hopping Spread Spectrum), která je upravena tak, aby mohla data přenášet. Modulace je založena na přeskakování mezi frekvencemi (anglicky hopping) — což znamenalo, že vysílač, který odeslal určitý úsek dat, změnil svoji frekvenci.

Samotné frekvenční pásmo 2,4 — 2,485 GHz bylo tím pádem zabráno jedním zařízením, které pracovalo s Wi-Fi technologií, jakékoliv další zařízení, jež bylo připojeno na Wi-Fi způsobovalo snížení kvality komunikace, a často docházelo ke kolizím. Dnes je pásmo rozděleno do třinácti kanálů a používá se především modulace OFDM. [10]

O dva roky později v roce 1999 došlo ke schválení dvou standardů IEEE 802.11a a IEEE 802.11b. Standard IEEE 802.11a zvládal na frekvenčním pásmu 5,4 GHz přenášet data o rychlosti 54 Mbit/s. Standard IEEE 802.11b začal být dostupný na nízkorozpočtových zařízeních a zachoval frekvenci 2,4 GHz, avšak nyní již při přenosové rychlosti 11 Mbit/s.

Firma Gartner v roce 2002 předpověděla masivní šíření technologie Wi-Fi pro následující rok. Technologie Wi-Fi se v roce 2003 skutečně začala zlevňovat a vznikl nový standard IEEE 802.11g, který nabízel rychlost přenosu dat až 54 Mbit/s v pásmu 2,4 GHz.

Od roku 2005 se na světových trzích drží dnes největší společnost vyrábějící bezdrátová síťová zařízení TP-Link. Společnost nyní funguje ve více než 100 zemích po celém světě. [11]

Po šesti leté odmlce, kterou způsobil masivní rozvoj technologií a honba za vyšší přenosovou rychlostí, se často stávalo, že jednotlivá zařízení nebyla vůbec mezi sebou kompatibilní. Z tohoto důvodu v roce 2011 vznikl nový standard 802.11n, standard navýšil přenosovou rychlost až na 150 Mbit/s.

V roce 2013 se objevil na trhu nový standard IEEE 802.11ac, který navýšil přenosovou rychlost až na 1 Gbit/s. [12]

Od roku 2014 je na trhu dostupný zatím posledně vydaný standard IEEE 802ad, standard pracuje s přenosovou rychlostí až 7 Gbit/s. [12]

3.3 IEEE 802.11

Standard byl vyvinut a je vyvíjen jedenáctou pracovní skupinou IEEE LAN / MAN standardizační komise (IEEE 802). Označení IEEE 802.11 je používáno pouze pro standard 802.11, který neobsahuje žádné další doplňky. Následné standardy obsahují množiny doplňků, pro standardy je využíváno označení 802.11x. Standard 802.11 zahrnuje šest druhů modulací pro posílání radiového signálu, přičemž všechny používají stejný protokol. Modulace jsou definovány v dodatcích označenými písmeny.

Přehled standardů IEEE 802.11				
Standard	**Rok vydání**	**Pásmo (GHz)**	**Maximální rychlost (Mbit/s)**	**Fyzická vrstva**
Původní IEEE 802.11	1997	5	54	OFDM
IEEE 802.11a	1999	5	54	OFDM
IEEE 802.11b	1999	2,4	11	DSSS
IEEE 802.11g	2003	2,4	54	OFDM
IEEE 802.11n	2009	2,4 nebo 5	nad 100	MIMO

Tabulka 1 Přehled standardů IEEE 802.11

3.3.1 IEEE 802.11a

Standard na rozdíl od standardů 802.11b a 802.11g pracuje ve frekvenčním pásmu 5,4 GHz, standard je schopen využívat pokročilý způsob modulace OFDM (Orthogonal Frequency Division Multiplexing) [14]. Z hlediska přenosu dat a stability zde došlo k výraznému pokroku z důvodu, že na této frekvenci nepracuje tolik zařízení, která by si mohla vzájemně rušit přenášený signál.

3.3.2 IEEE 802.11b

Standard byl dříve nejrozšířenější, dnes je již nahrazen standardem 802.11g, standardy jsou vzájemně kompatibilní. Standard 802.11b pracuje na frekvenčním pásmu 2,4 GHz s fyzickou vrstvou DSSS (Direct Sequence Spread Spectrum) [14] Nevýhoda tohoto standardu je poměrně nízká přenosová rychlost na dnešní požadavky. Maximální přenosová rychlost činí 11 Mbit/s.

3.3.3 IEEE 802.11g

Standard lze stále považovat za nejrozšířenější protokol Wi-Fi. Standard pracuje ve frekvenčním pásmu 2,4 GHz, je zpětně kompatibilní k IEEE 802.11b, avšak s tím rozdílem, že využívá OFDM (Orthogonal Frequency Division Multiplexing) [14] modulaci pro rychlosti 6, 9, 12, 18, 24, 36, 48 a 54 Mbit/s a pro rychlosti 1, 2, 5,5 a 11 Mbit/s používá totožné schéma jako pro standard IEEE 802.11b.

3.3.4 IEEE 802.11n

Standard si klade za cíl upravovat fyzickou vrstvu a podčást linkové, tzv. MAC (Media Access Control), aby docílil reálné přenosové rychlosti přes 100 Mbit/s. Navýšení rychlosti je docíleno použitím technologie MIMO (Multiple Input Multiple Output) [14], technologie využívá více vysílačů a přijímačů, aby byl navýšen dosah.

3.4 Režimy provozu

Režimy provozu Wi-Fi sítí umožňují vzájemně mezi sebou propojit dvě a více zařízení, která mohou spolu komunikovat, a to buď přímo (režimem Ad-hoc), nebo mohou společně komunikovat přes tzv. přístupový bod (Access Point, zkratka AP), to znamená, že jednotlivá zařízení spolu nikdy nekomunikují přímo, ale veškerá komunikace vždy prochází přístupovým bodem.

3.4.1 Režim infrastruktury

Většina Wi-Fi sítí funguje v režimu infrastruktury (Infrastructure Mode). Jednotlivá zařízení společně komunikují přes přístupový bod (AP). Pro správnou funkci sítě je zapotřebí, aby jednotlivá zařízení v okruhu příjmu signálu přistupovala nejméně k jednomu přístupovému bodu. Jednotlivé přístupové body vysílají v určitém časovém intervalu SSID (Service Set IDentifier) — programy na straně stanic, detekují dostupnost různých bezdrátových sítí a jsou identifikovány právě pomocí těchto identifikátorů. [2]

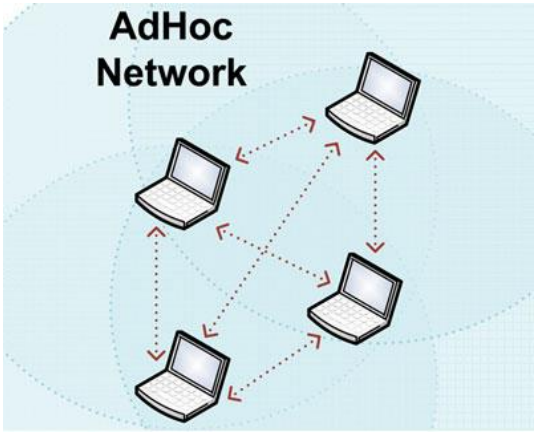
Příklad: V místnosti jsou dvě zařízení (notebooky), která jsou připojena do stejné bezdrátové sítě, i když fyzicky jsou zařízení přímo vedle sebe, tak spolu nekomunikují přímo. Komunikace mezi zařízeními probíhá nepřímo pomocí přístupového bodu. Jednotlivá zařízení vysílají pakety dat na přístupový bod, například router, který pakety dat následně odešle na jiná zařízení.

Obrázek 6 Režim infrastruktury, zdroj: http://cz.tp-link.com/article/?faqid=252

3.4.2 Režim Ad-hoc

Režimu Ad-hoc se také říká režim „Peer-to-Peer“. Režim bezdrátových sítí na rozdíl od režimu infrastruktury nevyžaduje žádný centralizovaný přístupový bod. Namísto toho zařízení v bezdrátové síti spolu přímo komunikují, avšak s nutností, aby jednotlivá zařízení byla v rádiovém dosahu ostatních zařízení, ke kterým se mají připojit.

Příklad: Dvě zařízení (notebooky), budou nastavena v režimu Ad-hoc, zařízení se připojí (spáruji) přímo na sebe bez nutnosti přístupového bodu.



Obrázek 7 Režim Ad-hoc, zdroj: http://www.bb-elec.com/Learning-Center/All-White-Papers/Serial/%E2%80%A2-Make-Your-Tablets-and-Smart-Phones-Smarter-Add-S.aspx

3.5 Výhody a nevýhody

- **Režim infrastruktury —** Režim je ideální pro vytvoření stále bezdrátové sítě. Bezdrátové směrovače zde fungují jako přístupové body, které mají obecně výkonnější bezdrátové vysílače a antény pro pokrytí širší oblasti na rozdíl od samotných zařízení, která nemusí mít tak výkonné vysílače a antény, aby umožnila kvalitní a stálý příjem signálu. [16]
- **Režim Ad-hoc —** Ad-hoc je výhodný při připojení pouze dvou zařízení bez nutnosti přístupového bodu. Nevýhodou režimu Ad-hoc je, že potřebuje více systémových prostředků, například fyzické rozložení sítě, které se vždy změní se závislostí na pohybu jednotlivých zařízeních. Je-li zapojeno mnoho zařízení v režimu Ad-hoc, bude existovat bezdrátové rušení, jelikož každé zařízení se musí přímo připojit k statním. Předávání dat pomocí několika počítačů je pomalejší než při využití přístupového bodu, přes který by data mohla bez rušení proudit. [16]

3.6 Útoky a hrozby

Každá síť může být napadena, neexistuje zcela bezpečná síť. To samé platí i o bezdrátových sítích, bezdrátové sítě jsou právě často napadány kvůli nedostatečnému zabezpečení proti útokům zvenčí, ale i zevnitř. Proto je nutné si uvědomit, že při komunikaci pomocí bezdrátové sítě jsou rádiové vlny volně šířeny vzduchem, které je možno snadně odposlechnout a získaná data zneužít. Podceněním bezpečnosti se uživatelé vystavují riziku odcizení, zničení, či modifikaci citlivých dat útočníkem.

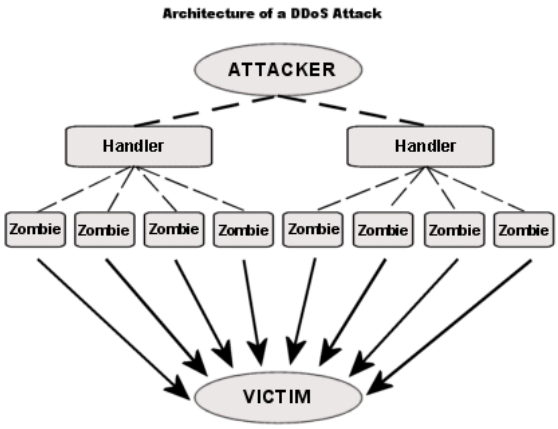
3.6.1 Odposlech

Zde se útočník zaměřuje na probíhající komunikaci mezi svými cíli, například mezi uživatelem a jeho bankou pomocí internetového bankovnictví. Při napadení může útočník buď pasivně odposlouchávat, nebo se stane aktivním prostředníkem, který komunikaci zprostředkuje.

- **Pasivní odposlech —** Útočník při této variantě odposlechu nasadí do napadeného počítače program, jenž zajistí, že síťový adaptér bude v promiskuitním režimu a zachytí veškerou komunikaci.
- **Aktivní odposlech —** Při použití aktivního odposlechu útočník odkloní síťový provoz a stane se aktivním prostředníkem, který komunikaci zprostředkuje. V důsledku slabého šifrování může získat klíč pro vstup do sítě, nebo může získat přístup pro nastavení přístupového bodu, kde může sledovat celkovou aktivitu na síti a následně útočit na ostatní zařízení.[1]

3.6.2 DoS

Hlavním úkolem DoS (Denial of Services) útoku je znemožnění přístupu na server, či přístupový bod tím, že útočník zasílá velké množství požadavků, které je server, v našem případě přístupový bod, nucen vykonat, například hromadné připojení velkého počtu zařízení k přístupovému bodu. Přístupový bod se stane v daném okamžiku nedostupný, to znamená, že není schopen v reálném čase odpovídat regulérním uživatelům, kteří se snaží přihlásit k přístupovému bodu. [19]



Obrázek 8 Schéma DDoS, zdroj: https://www.quora.com/How-does-one-perform-a-DDoS-attack

3.6.3 Man in the Middle

Je druh kybernetického útoku, při kterém útočník vstupuje přímo do systému, kde se stává součástí sítě. Snahou útočníka je odposlech komunikace mezi jednotlivými účastníky, přičemž se stane jejich aktivním prostředníkem. V rámci Wi-Fi sítí se jedná o to, že se útočník snaží oklamat uživatele a přístupové body, na které jednotliví uživatelé přistupují. Zde se útočník snaží vystupovat jako přístupový bod, ke kterému uživatelé běžně přistupují. Z pohledu přístupového bodu se útočník snaží jevit jako oprávněný uživatel, který má dostatečná práva k přístupu. [1]

Útočník tímto způsobem odposlouchává komunikaci a ze zjištění MAC adres dvou síťových zařízení mu umožní nahradit MAC adresu přístupového bodu za svoji. Tím zmate uživatele, že jeho zařízení se jeví jako „opravdový“ přístupový bod, ke kterému běžně přistupuje. To samé platí pro stranu přístupového bodu, kde se útočník snaží nahradit klientovu MAC adresu za svoji, aby mohl k němu přistoupit jako oprávněný uživatel. Cílem útočníka je snaha o to, aby komunikace na síti probíhala přes něj a on tím získal úplný přehled o veškeré komunikaci na síti.

Obrázek 9 Man in the Middle; zdroj: http://blog.privatewifi.com/csid-recommends-using-a-vpn-to-stop-man-in-the-middle-attacks/

3.6.4 Útok hrubou silou

Útok hrubou silou (Brute-Force Attack) vychází z testování různých možných kombinací hesla a uživatelského jména, což je časově velice náročné, avšak po určitém počtu pokusů a uplynutí potřebného času pro zjištění správné kombinace hesla a uživatelského jména dochází k jejich objevení. Plná automatizace útoku zapříčinila, že z prolomení kombinace hesla a uživatelského jména se stává pouze otázka času, než se útočníkovi podaří použít dostatečně spolehlivý algoritmus, který prolomí uživatelovu kombinaci hesla a uživatelského jména. Útoku hrubou silou velice napomáhají samotní

uživatelé, a to z prostého důvodu, že si volí velice jednoduchá a snadno prolomitelná hesla, například Heslo123, HesloHeslo, aj. Útok hrubou silou může být kombinován se slovníkovým útokem, kde jsou doplňována známa slova s dalšími možnostmi. [1]

A to je důvod, proč je v mnoha firmách využívána tzv. politika hesel, která se snaží zamezit možnému prolomení hesla (viz následná podkapitola: „Bezpečnostní služby v sítích“)

3.7 Bezpečnost sítě

V rámci bezpečnosti sítě jde o snahu minimalizovat zranitelnost jednotlivých síťových prostředků. Uživatelská data, služby, zařízení a samotní uživatelé potřebují ochranu, například proti zničení, poškození, či odcizení citlivých informací, která by mohla vést k poškození dobrého jména osoby (firmy). Síť může být ohrožena úmyslně (přímé poškození podnikajícího subjektu), neúmyslně (nedostatečná opatrnost uživatele na síti), útoky na síť mohou být vedeny zvenčí, taktéž zevnitř sítě. Pro navýšení bezpečnosti sítě je třeba použít správnou bezpečnostní politiku.

Bezpečnostní politika je souhrn komplexního zabezpečení, například fyzická bezpečnost, zálohování a archivace dat, zabezpečení před viry a malware, patch management aj. Bezpečnostní politiku si každá firma definuje sama v souladu se zaměřením společnosti a jejími finančními prostředky, jelikož stoprocentní bezpečnost společnosti je velice nákladná záležitost, proto se hledá kompromis mezi cenou a silou zabezpečení

3.7.1 Bezpečnostní služby v sítích

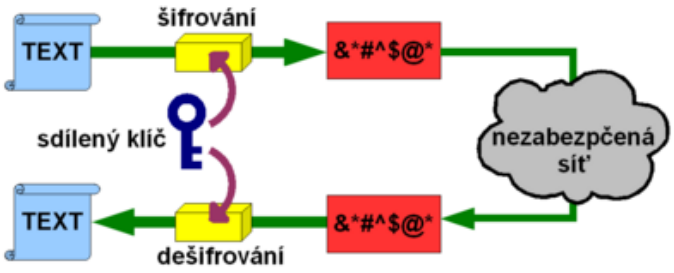
- **Autentizace —** Ověřuje totožnost druhé komunikující strany.
- **Řízení přístupu —** Identifikace uživatele na základě přidělených práv, která umožňují přístup do systému.
- **Zajištění utajení a důvěrnosti přenášených dat —** Ochrana před únikem informací (znemožnění odposlechu přenášené zprávy během přenosu, v případě, že se útočník snaží o odposlech, získaná data nebudou relevantní).
- **Zabezpečení integrity dat —** Zamezení neoprávněné změně, duplikaci, nebo poškození posílaných dat.
- **Ochrana proti odmítnutí původní zprávy —** Zabrání odesílateli, nebo příjemci odmítnout potvrzení o převzetí, nebo odeslání zprávy.

- **Politika hesel —** Politika hesel je bezpečnostní služba, kterou si definuje každá společnost sama na základě možného prolomení hesla uživatelů, například velká a malá písmena, speciální znaky, číslice, přesný počet znaků. Dále zajišťuje periodickou obměnu hesla.
- **Patch management —** Patch management zajišťuje, že bude provozovaný software neustále aktuální, to zahrnuje bezpečnostní záplaty operačních a jiných systémů, které zajistí minimalizaci možných napadaní. [20]

3.7.2 Šifrování

Šifrování je přeměna dat, která odesílané informace přetvoří do takové podoby, aby nedošlo k jejich případnému zneužít třetí osobu proti vůli odesílatele a příjemce. Tím je docíleno důvěrnosti přenášených dat.

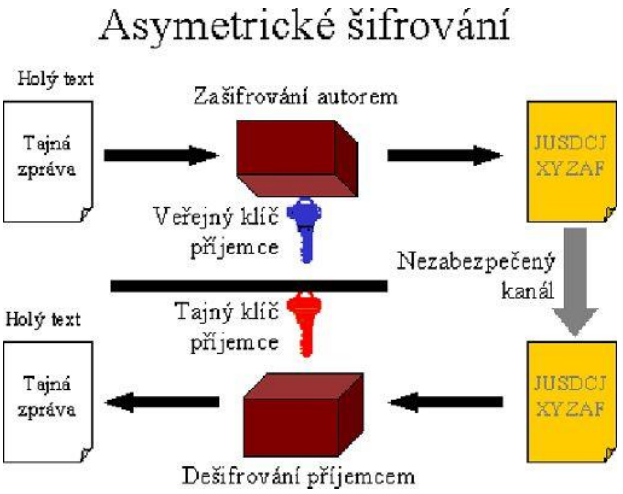
- **Symetrické šifrování —** Symetrické šifrování využívá soukromého klíče, který je použit při komunikaci obou stran. Klíč je sdílen stranami mezi sebou a je používán symetricky během šifrování dat i při jejich dešifrování. Symetrické šifrování je možno použít pro autentizaci i pro ochranu dat během přenosu. Avšak kvůli distribuci soukromého klíče vzniká požadavek na zabezpečení samotného klíče během přenosu sítí. Požadavek na zabezpečení samotného klíče zapříčinil jeho častou obměnu, aby nedošlo k případnému zneužití útočníkem [21].
- **DES (Data Encryption Standard 1977) —** Zde je použit 56 bitový klíč na blok dat o délce 64 bitů (každý osmý bit se používá jako parita). Způsob šifrování DES byl rozluštěn v roce 1997. Dnes je použit 3DES, který vylepšuje původní DES o jeho trojité použití [22].
- **AES (Advanced Encryption Standard 1997) —** AES používá dvě délky klíčů, a to 128, nebo 256 bitů. Klíče jsou použity k šifrování bloků dat o délkách 128, 192, 256 bitů. Všechny kombinace délek klíčů a šifrovaných bloků jsou možné. AES nabízí o 1021 více 128 bitových klíčů než DES. V roce 2001 nahradil DES a stal se normou FIPS (Federal Information Processing Standard). [22]



Obrázek 10 Symetrické šifrování; zdroj: https://kore.fi.muni.cz/wiki/images/thumb/9/97/Symetric_crypto.png/400px-Symetric_crypto.png

- **Asymetrické šifrování —** Asymetrické šifrování využívá veřejného klíče, to znamená, že data jsou šifrována jedním klíčem a mohou být dešifrována klíčem jiným. Avšak klíče vzájemně tvoří pár, kde jeden klíč odkazuje na druhý. Jedná se o klíče soukromé a veřejné. Soukromý klíč je znám pouze vlastníkovi, na rozdíl od veřejného klíče, který je dostupný všem. Asymetrické šifrování slouží především k ochraně přenášených dat, ale neslouží k autentizaci z důvodu znalosti veřejného klíče. Bohužel, nevýhodou šifrování pomocí veřejného klíče je složitost algoritmu, jenž slouží pro jeho zašifrování. Rychlost pro zašifrování přenášené zprávy u šifrování za použití soukromého klíče je mnohem rychlejší. Tento důvod vede k častému použití jejich vzájemné kombinace.

Příkladem asymetrického šifrování je **RSA**, kde spolehlivost je závislá na délce klíče, délka klíče zvyšuje bezpečnost a minimalizuje možnost dešifrování [22].



Obrázek 11 Asymetrické šifrování; zdroj: http://www.512.cz/images/7/70/Asymetricke-sifrovani.jpg

3.8 Zabezpečení Wi-Fi sítě

Je snaha o to, aby se minimalizovali, či úplně elimininovali možnosti přístupu neoprávněných uživatelů, kteří by v rámci firemní, či domácí sítě mohli odcizit, nebo jinak poškodit citlivá data uživatelů.

3.8.1 Skrytí SSID

Jedná se o vlastní název Wi-Fi sítě, SSID (Service Set Identifier) umožňuje, aby jednotlivá zařízení se mohla přihlašovat k přístupovému bodu[23]. V továrním nastavení routeru bývá zpravidla nastaveno, aby router svoje SSID vysílal v pravidelných intervalech, čímž oznamuje zařízením v síti, že se mohou na přístupový bod přihlásit. Přístupový bod se ohlašuje všem uživatelům, včetně případných útočníků, kteří ze znalosti SSID se mohou do nezabezpečené sítě přihlásit.

Přístupový bod je možno nakonfigurovat tak, aby nevysílal svoje SSID a zároveň, aby byl označen jiným názvem než továrním, jenž mu byl přidělen ve výrobě. Změnou SSID se ztíží možná identifikace a případné připojení útočníka k přístupovému bodu.

Po vypnutí SSID se daná síť přestane zobrazovat v seznamu dostupných bezdrátových sítí, která zařízení v okolí vidí, avšak přístupový bod stále vysílá své SSID při přihlašování zařízení na přístupový bod. V tento okamžik může připravený útočník odposlechnout SSID sítě.

3.8.2 WEP

WEP (Wired Equivalent Privacy) je soukromí ekvivalentní drátovým sítím, což představuje doslovný překlad samotného názvu [23]. Zabezpečení bylo vytvořeno jako součást standardu IEEE 802.11b. Protokol WEP se snažil dosáhnout totožné úrovně zabezpečení jako stíněné kroucené dvojlinky. Z důvodu přenosu dat vzduchem, je možný odposlech velmi snadný.

Protokol WEP je založen na šifrovacím algoritmu **RC4** (kryptografický algoritmus, který pracuje s náhodnou posloupností, posloupnost je sloučena s daty pomocí logické operace XOR). Algoritmus pracuje s tajným statickým klíčem o velikostech 40 nebo 104 bitů s 24 bitovým inicializačním vektorem (IV). WEP používá pro ověření integrity metodu **CRC-32** kontrolního součtu [20].

Implementace šifry **RC4** byla použita z důvodu jednoduché použitelnosti v rámci aplikací. Rychlost a jednoduchost, zapříčinily snadné využití v oblasti hardware, ale i software.

Protokol WEP byl prolomen v roce 2001, z tohoto důvodu mělo být nahrazeno zabezpečením pomoci WPA2 dle standardu IEEE 802.11i.

- **Autentizace —** Jednostranná autentizace představuje u protokolu WEP obrovskou nevýhodu, protože uživatel neví, zda přistupuje k autorizovanému přístupovému bodu. Autentizace probíhá pouze na úrovni zařízení, ne však na úrovni uživatelů, to znamená, že při odcizení zařízení je potřeba přenastavit klíč na všech zařízeních [20].
- **Šifrování —** Nevýhoda šifrování tkví v použití stejného (sdíleného) klíče na všech zařízeních Wi-Fi. Statický klíč o velikosti 24 bitů je měněn při každém paketu, avšak během běžného provozu dochází k jeho opakování v závislosti na šifrovacím mechanismu **RC4**. Distribuce klíčů musí být prováděna manuálně [20].

3.8.3 WEP2

Vylepšení původního WEP zabezpečení. Cílem protokolu bylo odstranit bezpečnostní chyby, které se týkaly inicializačních vektorů. WEP2 rozšířil inicializační vektory a zesílil šifrování na 128 bitové. Bezpečnostní problémy zůstaly nezměněny a jsou totožné se zabezpečením WEP. Prolomení zabezpečení útočníkovi zabere pouze více času než u WEP [24].

3.8.4 WPA

Z důvodu nedostatečného zabezpečení pomocí WEP, které bylo v roce 2001 prolomeno. Vzešel požadavek na nové řešení, aby původní zabezpečení nahradilo. Roku 2002 vydala asociace Wi-Fi Alliance WPA (Wi-Fi Protected Access), které bylo zamýšleno jako dočasné řešení před příchodem normy 802.11i. WPA je zpětně kompatibilní s WEP, a to díky RC4 šifře. WPA je dopředně kompatibilní s normou 802.11i.

Podstatnými změnami WPA od WEP je odstranění nulové autentizace a nepoužití šifrování pomocí statického klíče. Namísto toho se používá pro šifrování dočasný klíč, který je obměňován technologií **TKIP** (Temporal Key Integrity Protocol), kde klíč je měněn dynamicky pomocí metody **MIC** (Message-Integrity Check). [20]

- **TKIP (Temporal Key Integrity Protocol) —** Hlavním cílem protokolu je dynamická správa šifrovaných klíčů mezi jednotlivými body, a to jak na začátku, tak i v průběhu komunikace, protokol kontroluje integritu zpráv a zároveň čísluje jednotlivé pakety na ochranu proti útokům typu Replay. [20]

- **MIC (Message-Integrity Check) —** Integrita dat je zajištěna kódem MIC. Jednotlivé rámce obdrží digitální podpis, který zamezuje útokům typu Man in the Middle. Podpis je automaticky vypočítáván ze základu datové části přenášeného rámce, včetně zdrojové a cílové MAC adresy, pořadového čísla paketu a náhodné hodnoty (tyto části jsou zabudovány do datové části rámce a následně zašifrovány). [20]

3.8.5 802.11i

Teprve až v červnu roku 2004 byl standard 802.11i (WPA2) normován asociací Wi-Fi Alliance, standard byl označen pod názvem WPA2. Od 13. března 2006 je certifikace WPA2 povinná pro všechna nová zařízení, která chtějí být certifikována jako Wi-Fi. WPA2 přidává protokol **CCMP** (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol), protokol pracuje na bázi silného šifrování **AES** (Advanced Encryption Standard), jež mění dynamicky 128 bitový klíč. [24]

WPA2 je zpětně kompatibilní se standardem WPA. WPA2 podporuje také TKIP, AES, WPA-PSK a 802.1x autentizované WPA sítě.

Základní změnami standardu IEEE 802.11i jsou například oddělování autentizace uživatele od vynucování integrity a soukromí zprávy, tím je zajištěna stabilita a velká škálovatelnost bezpečnostní architektury, která není jen určena pro domácí sítě.

Architektura 802.11i pro bezdrátové sítě je označena **RSN** (Robust Security Network). **RSN** slouží pro autentizaci, silnou distribuci klíčů a nové mechanismy k zajištění integrity a soukromí. Architektura **RSN** je složitější, avšak nabízí bezpečné a rozšiřitelné řešení pro bezdrátovou komunikaci. Bohužel, ve většině případů akceptuje **RSN** pouze zařízení, jež podporují **RSN**. Standard IEEE 802.11i definuje architekturu **TSN** (Transitional Security Network), do které je možno zahrnout jak systémy **RSN**, tak i systémy WEP. Pokud autentizace nebo asociace používá mezi zařízeními čtyř fázový handshake, tak se asociace označuje jako **RSNA** (Robust Security Network Association).

Sestavení bezpečného komunikační kontextu se skládá ze čtyř fází:

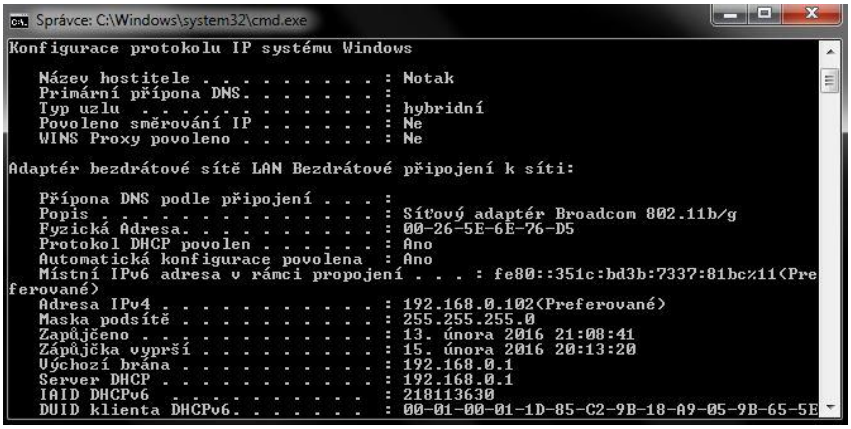
1. Odsouhlasení bezpečnostních zásad
2. Autentizace 802.1x
3. Odvození a distribuce klíče
4. Utajení a integrita dat RSNA

3.8.6 Filtrace MAC adres

MAC adresa je unikátní číslo složeno z hexadecimální kombinace čísel, která obdrží síťová karta, nebo jiné zařízení již ve výrobě. Filtrace MAC adres umožňuje správu přihlášených zařízení k Wi-Fi routeru, jež byly zadány ručně do paměti routeru. Při přihlášení zařízení na router je rozpoznáno, zda bylo zahrnuto do seznamu povolených zařízení pro přístup. Při přenosu dat ze zařízení na router, není MAC adresa šifrována, a to i za podmínky, že využíváme techniku šifrování jako WEP, WPA, a jiné. [25]

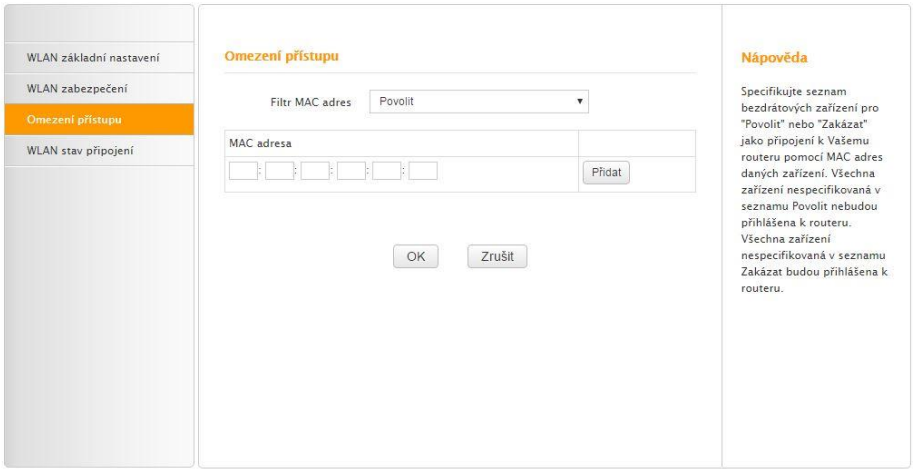
Příklad: Ukázka filtrace MAC adres na routeru Tenda W311R+ za pomocí operačního systému Windows 7 Professional. V ukázce budou přeskočeny prvky, jako například přihlášení na router a následná proklikání nabídkou do vybrání podnabídky „Omezení přístupu“.

Jako první bude spuštěna příkazová řádka pomocí příkazu **cmd**, do příkazové řádky je nutné zadat jednoduchý příkaz **ipconfig /all**, který vypíše IP adresu zařízení, masku sítě a výchozí bránu, přes kterou zařízení přistupuje na Internet.



Obrázek 12 CMD; zdroj: Příkazová řádka, vlastní pozorování

Hodnota výchozí brány je 192.168.0.1, tuto hodnotu je potřebné si opsat a zadat ji do jakéhokoliv prohlížeče. Z nabídek v routeru je třeba vybrat podnabídku s názvem: „Omezení přístupu“ viz obrázek níže.



Obrázek 13 Omezení přístupu; zdroj: Nastavení routeru, vlastní pozorování

Podnabídka „Omezení přístupu“ nabízí možnost buď filtraci povolit, či zakázat. Omezit přístup je umožněno jednotlivým zařízením, která na základě MAC adresy lze zahrnout do seznamu povolených, nebo zakázaných zařízení.

3.8.7 VPN

Virtuální privátní sítě umožňují uživatelům bezpečně přistupovat k privátní datovým sítí, které jsou vzájemně propojeny dohromady přes nezabezpečenou veřejnou síť. Cílem je dosažení stavu, kdy jednotlivá zařízení budou společně komunikovat, jako by byly propojeny v rámci jedné fyzické sítě. Řešení využívají podniky z důvodu zabezpečení citlivých dat, která mohou být uložena u klientů. V dnešní době jsou VPN (Virtual Private Network) taktéž často využívány v domácnostech. VPN využívají kombinaci šifrovacích protokolů a ověřených připojení pro generování P2P (Peer-to-Peer) připojení. [26]

Bezpečnostní protokoly:

- **IPSec (IP Security) —** Internetová komunikace je často zabezpečena pomocí protokolu IPsec, který může pracovat ve dvou režimech. Transportní režim šifruje pouze datový paket, za to v režimu tunelování je šifrován celý datový paket. [27]
- **SSL (Secure Sockets Layer) a TLS (Transport Layer Security) —** SSL a TLS jsou často používány v oblastech, které zahrnují on-line prodej, či poskytování služeb. SSL je založeno na protokolu http a je vždy iniciováno stranou klienta ve formě URL adresy začínající https://. Na začátku této relace je vždy proveden SSL handshake, aby produkoval kryptografické parametry relace. Parametry jsou typické pro digitální certifikáty. Jedná se o prostředky pro výměnu šifrovacích klíčů, ověření relace a následné vytvoření zabezpečeného připojení. [27]

- **PPTP (Point-to-Point Tunneling Protocol) —** PPTP je používán od poloviny roku 1990. PPTP nemá šifrování, pouze do jednotlivých tunelů zapouzdřuje datové pakety. Sekundární protokoly, jako GRE, nebo TCP musí být použity pro zpracování šifrování. Úroveň zabezpečení PPTP byla již předčena novějšími metodami, avšak protokol zůstal silný, i když není nejbezpečnějším. [27]
- **SSH (Secure Shell) —** Protokol SSH je schopen vytvořit tunel pro VPN a jeho následné šifrování. SSH umožnil uživatelům přenášet nechráněná data ze serverů prostřednictvím šifrovaného kanálu. Z toho vyplývá, že data nejsou šifrována, nýbrž kanál, který data přenáší, je zašifrován. Připojení SSH vytváří SSH klienta, jenž předává data z lokálního portu na port vzdáleného serveru. [27]

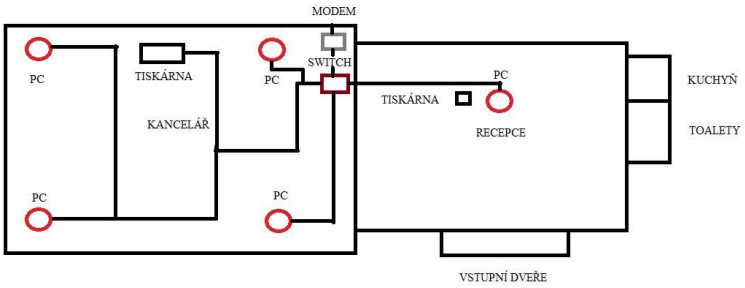
4 Vlastní řešení

Praktická část bakalářské práce popisuje návrh zabezpečení bezdrátové sítě na základě získaných dosavadních poznatků, jež byly zpracovány v teoretické části. Bakalářská práce hodnotí zabezpečení fiktivního podniku, který se zabývá účetnictvím a daněmi. Fiktivní společnost je vystavěna na poznatcích z reálného podniku. Práce by měla popisovat zabezpečení bezdrátové sítě reálné firmy, avšak popis zabezpečení firemní sítě nebyl umožněn dle § 40 odst. 1 zákona č. 262/2006 Sb., z důvodu možného vynášení informací třetí straně.

Firma požaduje, aby její zabezpečení sítě bylo cenově přijatelné, z důvodu malé velikosti firmy, která nově vstoupila na pracovní trh a v blízké době neočekává rychlý rozvoj. Společnost si pronajala prostory v obytné budově, jako kancelář, kde byly vystavěny prostory pro „rodinnou“ firmu. Podnik ke své práci používá čtyři přenosné počítače, včetně dokovacích stanic pro zařízení. K dokovacím stanicím jsou připojeny běžné periferie jako myš, klávesnice a monitor. Recepce využívá jedné pracovní stanice s příslušnými periferiemi, k pracovní stanici je instalována černobílá laserová tiskárna napojena přes USB port, ve velké kanceláři se nachází barevná laserová tiskárna, která je sdílena pomocí sítě.

4.1 LAN

Řešení pomocí centralizace switche by bylo velmi nákladné a pro tuto firmu velice nepraktické, z důvodu nízkého počtu „pevných“ zařízení, která jsou využívána uvnitř společnosti. Poskytovatelem Internetu je společnost O2. Firma O2 dodala modem VDSL ZyXEL VMG1312-B30B, k modemu je navázán switch s firewallem Netgear FVS318N, ke kterému přistupují jednotlivá zařízení. Vnitřní síť LAN tedy funguje jako hvězdicová topologie. Viz obrázek níže.



Obrázek 14 Rozvod kabeláže; zdroj: vlastní pozorování

4.2 Wi-Fi

Router Netgear FVS318N pracuje jako bezdrátový směrovač, jenž umožňuje výměnu dat a informací mezi dvěma sítěmi. Ke směrovači přistupují jednotlivá bezdrátová, ale také i drátová zařízení. Směrovače mají za úkol řídit síťový provoz. Směrovače můžeme rozdělit na drátové nebo bezdrátové. Směrovače mohou obsahovat také Firewall jako výše zmíněný Netgear FVS318N.

4.2.1 Nastavení bezdrátové sítě

Nastavení bezdrátové sítě bylo pozměněno, z důvodu navýšení bezpečnosti jednotlivých zařízení uvnitř sítě, změna se týká například typu šifrování, které bylo nastaveno ve výrobě na WPA. Nyní již router pracuje na pokročilém typu zabezpečení 802.11i (WPA2) s podporou šifrování AES. Navíc došlo ke změně sdíleného klíče na více znakový z původního Password123. Filtr MAC adres byl nastaven pouze pro přístup zařízení v rámci společnosti.

4.2.2 Nastavení Firewallu

Uvnitř nastavení Firewallu lze nastavit URL filter, jenž zamezuje pracovníkům přístup na stránky s nevhodným obsahem, jako například stránky, které podporují rasismus, sexuální kontext, nebo jakékoliv stránky, nesouvisející s náplní práce. V nastavení je možnost vyfiltrovat specifická slova, to znamená, že v daném routeru je zabudován filtr klíčových slov. Filtr zamezuje přístup na webové stránky, které mohou obsahovat nevhodná slova, jako například xenofobie, násilí, aj.

V rámci nastavení Firewallu je možnost nastavit Filtr síťových služeb, filtr umožní zablokování výměny paketů ze sítě LAN do sítě WAN, a také zamezí jednotlivým zařízením v síti využití síťových služeb.

Příklad: Blokování síťové služby HTTP, služba funguje na portu 80, tím je docíleno toho, že uživatel na dané stanici nebude moci vůbec přistupovat k Internetu, a to celé za podmínky, že byla vyplněna konkrétní IP adresa počítače. Pokud konkrétní IP adresa počítače není uvedena, omezení bude platit na všechna zařízení v sítí.

4.3 WAN

Sítě WAN i LAN jsou od sebe vzájemně odděleny pomocí modemu a routeru. Na straně routeru byly nastaveny Access Control Lists.

Access Control Lists [28], jsou seznamy, které řídí, zda jsou pakety přijaty, nebo zablokovány na rozhraní routeru, a to na základě kritérií, které byly definovány při vytváření seznamu řízeného přístupu. Jednotlivé pakety jsou čteny po řádcích, dokud se nenarazí na shodu, následně je paket přijat nebo odmítnut v závislosti na nastavení kritéria, následné řádky paketu již nejsou nadále čteny.

Příklad: ACL číslo 105 popisuje přístup na server 10.5.1.10 odkudkoliv, avšak nastavení je omezeno pouze pro port číslo 80, port slouží pro práci s HTTP, ping IP adresy serveru je umožněn.

Příklad byl převzat z [29]

SWITCH (config)#access-list 105 permit tcp any host 10.5.1.10 eq 80

SWITCH (config)#access-list 105 permit icmp any any echo

SWITCH (config)#access-list 105 permit icmp any any echo-reply

SWITCH (config)#access-list 105 deny ip any any

4.4 Možná řešení zabezpečení

Nynější sekce bakalářské práce bude hodnotit současné řešení zabezpečení společnosti a možná další řešení zabezpečení při následném vývoji z „rodinné firmy“ na firmu malého, nebo středního rozsahu.

4.4.1 Zabezpečení pomocí MAC adres

Zabezpečení pomocí filtrace MAC adres je jedno z možných základních zabezpečení, jak zabezpečit firemní, či domácí sít. Principem tohoto zabezpečení je, že administrátor musí jednotlivá zařízení přidávat do filtru MAC adres, která se mohou připojit k síti. To znamená, že každé zařízení, které chce přistupovat na Internet, musí být

zahrnuto v seznamu povolených MAC adres. Pokud zařízení není zahrnuto ve filtru MAC adres, přístup zařízení bude odepřen.

V malé firmě má toto zabezpečení velký význam a z důvodu snadného přehledu zařízení, která jsou připojena do místní sítě. Bohužel, při možné budoucí expanzi firmy, nastane situace, kdy se počet zařízení navýší uvnitř firemní sítě a zařízení budou muset být ručně přidána do databáze routeru, aby mohla přistupovat k Internetu. Řešení pomocí filtrace MAC adrese se stává velice nepraktickým, protože administrátor je nucen jednotlivá zařízení přidávat ručně.

Slabinou tohoto zabezpečení je snadná možnost odposlechu přenášených dat mezi jednotlivými zařízeními, kde je přenášena MAC adresa, která je přes možné zabezpečení pomocí WPA snadno zachytitelná. Pokud MAC adresa byla útočníkem odposlechnuta, útočník může upravit svoji MAC adresu zařízení, aby vypadala jako validní MAC adresa zařízení, které může přistupovat do vnitřní sítě.

4.4.2 Zabezpečení pomocí VPN

Zabezpečení pomocí VPN zajišťuje komunikaci mezi zařízeními pomocí veřejné sítě, kde oboustranná komunikace je zajištěna pomocí zabezpečené privátní sítě. Principem tohoto zabezpečení je, že se vytvoří šifrovaný tunel mezi klientem a VPN serverem, kde bude veškerá komunikace vedena tímto tunelem.

Řešení v rámci fiktivní firmy může být využito z důvodu umožnění vzdáleného přístupu z domova, nebo ke klientovi, kde by poskytované služby byly nabízeny externím dodavatel. Pro současný i budoucí stav firmy je řešení pomocí VPN velice pozitivní, z důvodu malých prostor společnosti a možného budoucího rozvoje firmy. Avšak s tímto řešením by bylo třeba pořídit novou infrastrukturu v podobě nového switche, jenž umožnuje zabezpečení pomocí protokolu PPTP, L2TP, aj. Nebo vytvoření vlastního VPN serveru, na který se budou klienti připojovat vzdáleně. Alternativou k řešením by mohlo být využití externího VPN poskytovatele, aby spravoval šifrovanou komunikaci a správu VPN tunelu.

Příkladem je zde uvedeno několik VPN poskytovatelů:

- **CyberGhost —** Při zabezpečení sítě poskytovatel VPN umožnuje výběr jedné sdílené statické IP adresy serveru, ke kterému se budou uživatelé připojovat. CyberGhost neumožňuje při připojení do VPN záznam IP adres nebo dat. Při používání softwaru OpenVPN nabízí poskytovatel možnost využívat zabezpečení AES, u šifrovacích protokolů L2TP/IPSec nabízí 256/128 šifrování. CyberGhost je kompatibilní pro zařízení, jež pracují na platformě Windows, MacOS, iOS, nebo Android. U ostatních systémů je VPN nutno nastavit ručně. Připojit lze až pět zařízení v závislosti na nakoupeném paušálu. Uživatelská podpora je momentálně velice nepříjemná z důvodu, že společnost v současném stavu garantuje odpověď na požadavky do třech pracovních dnů, a to pouze v rámci pracovní doby. [30]

  Cena nabízeného řešení za pět zařízení činí 95,88 € ročně, v přepočtu na české koruny cena nabízeného řešení je 2111 CZE bez DPH za rok. [31]

- **IPVanish —** Poskytovatel VPN nabízí možnost, že jeho jednotlivé servery mají dynamické IP adresy, ke kterým se mohou uživatelé připojit. Opět jako u CyberGhost IPVanish nezaznamenává naše aktivity. Poskytovatel nabízí možnost připojení dvou zařízení najednou přes VPN. IPVanish využívá protokolů OpenVPN, nebo L2TP/IPSec. Obdobně jako u CyberGhost ani IPVanish nemá podporu 24/7, podpora probíhá pouze v pracovní dny během standardní pracovní doby. [30]

  Cena nabízeného řešení činí 77,99 $ ročně, v přepočtu na české koruny je cena nabízeného řešení 1914 CZE bez DPH za rok. [32]

- **TorGuard —** TorGuard nabízí sdílené IP adresy serverů, avšak vždy jedna IP adresa připadá na jeden server. Při příplatku je možno využít dedikované IP adresy. Jako u předchozích poskytovatelů ani TorGuard nezaznamenává naše aktivity. Poskytovatel nabízí možnost připojení přes protokoly OpenVPN, PPTP, L2TP.

  TorGuard na rozdíl od předchozích poskytovatelů nabízí uživatelskou podporu 24/7 a možnost připojit až pět zařízení najednou, k dalším zařízením je nutno dokoupit licenci, která stojí 1$ / zařízení. [30]

  Cena nabízeného řešení činí 119,88 $ ročně, v přepočtu na české koruny cena nabízeného řešení je 2942 CZE bez DPH za rok. [33]

- **Vlastní řešení —** Při použití vlastního řešení můžeme sami rozhodovat o tom, jaká zařízení budou k VPN serverům přistupovat, na rozdíl od dodavatelského řešení, kde bychom mohli VPN server sdílet s ostatními uživateli dodavatele. Pro společnost by bylo nesmyslné zřizovat přímo dedikovaný VPN server z důvodu nákladovosti a momentálního využití. Řešení pomocí VPN serveru je vhodné pro mnohem větší společnost, například s patnácti a více zařízeními včetně zařízení, která se budou připojovat z domácího prostředí do intranetu společnosti.

Pro současné řešení firemní sítě a současnou velikost společnosti je doporučeno řešení pomocí VPN routeru Cisco RV325, router obsahuje přímo zabudovanou VPN, včetně Firewallu a možnosti využití protokolů IPSec, nebo PTP.

Jednorázová cena pořízení routeru činí 6442 bez DPH. K ceně routeru je nutno započíst měsíční sazbu administrátora lokální sítě, jenž bude zodpovídat za provoz VPN routeru a jiných zařízení uvnitř firemní sítě, sazba administrátora činí 20000 CZE hrubého.

Uživatelská podpora bude na vysoké úrovni z důvodu okamžitého zásahu lokálního administrátora společnosti, administrátor může okamžitě přistoupit k routeru a řešit možný problém s připojením. Funkčnost uživatelské podpory je zajištěna po celý týden, a to včetně víkendů a svátků, kdy se jednotliví administrátoři střídají po týdenních cyklech.

4.4.3 Zabezpečení pomocí RADIUS serveru

Dalším možným řešením pro společnost je využití protokolu RADIUS (Remote Authentication Dial In User Service). Protokol pracuje na architektuře klient—server, kde častými klienty protokolu RADIUS jsou NAS (Network Access Server), klienti jsou často zpodobněni uvnitř sítě, například routery, huby, anebo switchy. RADIUS server zajišťuje autentizaci (ověření identity uživatele pomocí jména a hesla) uživatelů, kteří se připojují do vnitřní sítě vzdáleně, autorizaci (oprávnění manipulace s daty, nebo službami v síti) a účtování, jež zajišťuje kontrolu a následný záznam aktivit po celou dobu připojení uživatele. Nejčastěji účtování využívají poskytovatelé Internetu pro vystavení faktur uživatelům za poskytnuté služby. [34]

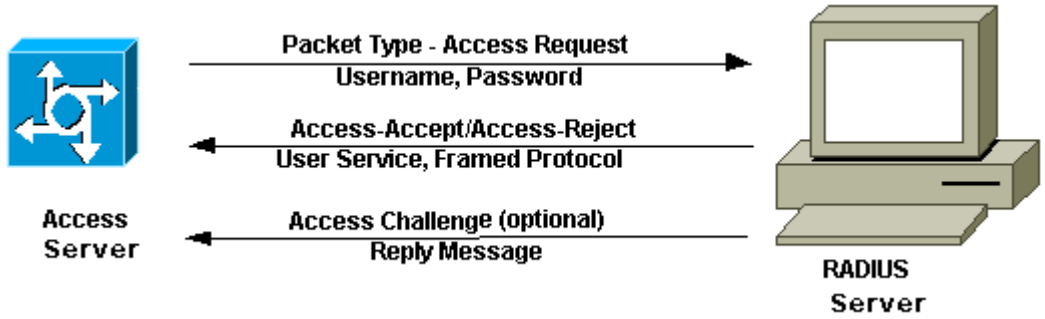
Příklad: Uživatel, který se přihlašuje do interní bezdrátové sítě, musí předat routeru své autentizační údaje (uživatelské jméno a heslo). Klient informace obdrží a pomocí RADIUS protokolu provede autentizaci uživatele na základě obdržených údajů. Při spuštění autentizace je vytvořen klientem tzv. Access-Request (v překladu požadavek

o přístup), uvnitř požadavku jsou atributy: uživatelské jméno, heslo, a číslo portu připojeného uživatele.

Odesláním požadavku o přístup na RADIUS server je zajištěno jeho přijetí RADIUS serverem. Server po obdržení požadavku prověří klienta, od kterého vzešel. Nezná-li RADIUS server klienta, bude klientský požadavek serverem zahozen a přístup klienta je odmítnut. Proběhne-li ověření klienta v pořádku, RADIUS server začne vyhledávat v databázi uživatelů, kde jsou uloženy informace o uživateli, například IP adresa zařízení, ze kterého se přihlašuje, aj. Tyto údaje musí souhlasit se všemi údaji, aby byl umožněn uživateli přístup do intranetu. Na základě přístupu je ověřeno heslo, pro specifikaci portu, nebo klienta, ke kterému je uživatel přihlášen. [35]

Obrázek níže popisuje, jak probíhá autentifikace a následná reakce RADIUS serveru, zda byl umožněn uživateli přístup. Po kladném vyřízení uživatel obdrží hlášku Access-Accept (v doslovném překladu přístup povolen), v opačném případě by uživatel obdržel chybovou hlášku Access-Reject (v doslovném překladu přístup zamítnut), kde je přístup odepřen.[36]

Obrázek je obohacen o Access Challenge (v doslovném překladu výzva k přístupu), jedná se o dodatečné poskytnutí informací od uživatele, které se mohou týkat zadání druhého heslo, nebo PINu, nebo tokenu, jenž uživatel pro přihlášení využívá.



Obrázek 15 RADIUS server; zdroj: http://www.cisco.com/c/dam/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32b.gif

4.5 Zhodnocení VPN poskytovatelů

Zhodnocení VPN poskytovatelů proběhne formou metody bodovací, která na základě výsledků vybere vhodné řešení pro současný a možný budoucí vývoj zabezpečení fiktivní společnosti. Metoda bodovací pracuje na principu výběru variant, kde jednotlivé varianty musí být vždy ohodnoceny na stejné bodovací stupnici, například od jedné do desíti. Cílem bodovací metody je, že nejlepší řešení obdrží největší počet bodů. Váhy kritérií udávají, jakému kritériu dává společnost přednost. Výběr preferencí je čistě subjektivní, aby vyhovoval nárokům společnosti. Tabulka níže popisuje jednotlivé vybrané varianty, které ovlivňují výběr vhodného řešení pro současný stav společnosti.

Zhodnocení VPN poskytovatelů					
	Počet možných připojených zařízení	**Podporované protokoly**	**Uživatelská podpora**	**Cena**	**Součet**
CyberGhost	4	6	2	7	5
IPVanish	2	6	4	9	5,7
TorGuard	6	6	7	6	7,1
Vlastní řešení	9	7	9	2	7,6
Váhy kritérii	0,2	0,1	0,5	0,3	

Tabulka 2 VPN poskytovatelé

Z výsledků tabulky vychází, že na prvním místě se umístilo řešení, které by si firma spravovala sama. Na základě bodovací metody a váženého součtu řešení obdrželo 7,6 bodů. Nabízí se možnost vysokého počtu připojených zařízení za pomoci VPN. Router Cisco RV325, umožňuje podporu protokolů PPTP, L2TP, IPSec a PPPoE. Uživatelská podpora je na vyšší úrovni než od společnosti TorGuard, protože by probíhala přímo na místě problému. Pro současný stav společnosti je toto řešení nákladné, avšak nutné, a to z důvodu najmutí správce sítě, který by spravoval VPN tunel, včetně dalších zařízení uvnitř společnosti.

V těsném závěru za vlastním řešením se umístilo řešení od společnosti TorGuard. Na základě bodovací metody a váženého součtu řešení obdrželo 7,1 bodů. Důvodem je vysoký počet zařízení, jež jsou připojena pomocí VPN, možnosti využití protokolů OpenVPN, PPTP, L2TP. Na rozdíl od vlastního řešení zde podpora probíhá pouze vzdáleně v anglickém jazyce. Řešení bylo také doporučeno pro současný stav a velikost společnosti, avšak za podmínky, že společnost již administrátora sítě má.

Na třetím místě tabulky se umístilo řešení od společnosti IPVanish, které obdrželo pomocí bodovací metody a váženého součtu 5,7 bodů. IPVanish nabízí nejlepší možnou cenovou nabídku za poskytované služby, avšak řešení má možnost pouze připojit dvě zařízení přes VPN, což je pro současný i možný budoucí rozvoj firmy nepraktické. Poskytovatel, jako předchozí, nabízí podporu třech protokolů: OpenVPN, L2TP a IPSec. Uživatelská podpora je na rozdíl od předchozích dvou řešení na nižší úrovni, kvůli podpoře, která je zajišťována pouze v pracovní dny po dobu pracovní doby.

Čtvrté a poslední místo tabulky obsadila společnost CyberGhost, které obdržela pomocí bodovací metody a váženého součtu 5 bodů. Řešení nabízí druhou nejlepší možnou cenovou nabídku za své služby, avšak nejhorší uživatelskou podporu z výše uvedených, a to kvůli dlouhé době na zpracování požadavku. V rámci řešení je možno připojit až pět zařízení najednou přes VPN. Pro současný stav by řešení od společnosti CyberGhost bylo dostačující, nýbrž pro budoucí vývoj by nebylo optimální, a tím pádem nesmyslné. Podporované protokoly jsou OpenVPN, L2TP a IPSec, jako u předchozích dvou řešení.

4.6 Doporučení vhodného řešení pro fiktivní společnost

Na základě předchozích šetření, která se zabývala možnostmi, jak zabezpečit bezdrátovou síť, včetně zhodnocení VPN poskytovatelů, kde firmě vzešel požadavek na zajištění správce sítě, firma požaduje, aby pro stávající velikost firmy bylo upřednostněno cenové hledisko před silou zabezpečení. Ale aby zabezpečení bylo stále na dostatečné úrovni.

Tabulka níže popisuje vhodná řešení pro fiktivní společnost, která byla vybrána na základě subjektivních preferencí společnosti.

	Preferenční tabulka				
	Cena pořízení	**Zásah administrátora**	**Nutnost přepracování sítě**	**Síla zabezpečení**	**Celkový počet**
Zabezpečení pomocí MAC adres	1	4	1	4	10
Zabezpečení pomocí VPN	3	3	2	2	10
Zabezpečení pomocí RADIUS	4	3	4	3	14
Zabezpečení pomocí kombinace MAC adres a RADIUS	5	4	4	1	14

Tabulka 3 Preferenční tabulka

Stupnice hodnocení:

1 — výborné

2 — velmi dobře

3 — dobře

4 — dostatečné

5 — nedostatečné

Čím je výsledný počet bodů vyšší, tím v současné situaci navrhované řešení nevyhovuje nárokům společnosti.

Z výsledků tabulky vychází dvě nejlepší možná řešení, která jsou stejně bodově ohodnocena. Jedná se o zabezpečení pomocí MAC adres a VPN, obě zabezpečení obdržela ohodnocení 10. Pokud bude firma preferovat cenové hledisko, je v současné chvíli lepší řešení pomocí filtrace MAC adres, avšak toto řešení nemusí být vždy dostačující proti případným útokům z vnější sítě. Z pohledu administrátora je řešení velmi „nepříjemné“, z důvodu neustálého přidávání nových zařízení do filtru MAC adres.

Pokud se firma zaměří na bezpečnostní hledisko, bude vyhovovat spíše varianta zabezpečení pomocí VPN. Pořizovací cena bude o něco vyšší, než zabezpečení pomocí MAC adres. Zásahy administrátora se na rozdíl od předchozího řešení sníží, avšak ne o tolik, protože administrátor, musí nakonfigurovat VPN tunel, případně kontrolovat stav VPN, zda je v provozu, či nikoliv. S využitím VPN tunelu vzroste zabezpečení komunikace po veřejné síti, což umožní uživatelům přistupovat z domácího prostředí do firmy.

Na třetím až čtvrtém místě se umístila opět dvě řešení, která jsou stejně bodově ohodnocena. Jedná se o zabezpečení pomocí RADIUS serveru a pomocí kombinace RADIUS serveru a zabezpečení pomocí filtru MAC adres, řešení obdržela 14 bodů. Bude-li firma preferovat pouze zabezpečení pomocí RADIUS serveru, cena pořízení pro současný stav společnosti je vyšší než firma požaduje, a to z důvodu nákupu dedikovaného zařízení, jež zajistí funkci RADIUS serveru, vzhledem k začlenění dedikovaného zařízení jako RADIUS serveru bude třeba celou síť přepracovat. Řešení potřebuje občasné zásahy administrátora pro provoz a přidávání autorizovaných uživatelů do databáze na RADIUS serveru. Síla zabezpečení je ohodnocena číslem tři, protože RADIUS server již neposkytuje další jiné zabezpečení než pouze ověření identity přihlašujícího uživatele.

Kombinace filtrace MAC adres a RADIUS serveru by byla vhodná, že by jednotlivá zařízení byla umístěna do povoleného filtru MAC adres a zároveň oprávnění uživatelé v databázi RADIUS serveru. Pokud by došlo k odcizení zařízení, které má nastavenou výjimku ve filtru MAC adres, útočník by mohl ze samotné znalosti MAC adresy přistoupit k vnitřní síti společnosti, avšak s kombinací pomocí RADIUS serveru musí útočník projít autorizací zařízení a uživatele, která by mu případný přístup

znemožnila. Z toho vyplývá, že řešení je z bezpečnostního hlediska nejlepší možné. Bohužel, řešení je pro současný stav společnosti velmi nákladné, v tuto chvíli preferuje spíše hledisko finanční než bezpečnostní. Zásahy administrátora by byly velmi vysoké, kvůli přidávání, či odebírání zařízení z filtru MAC adres a následného přidávání uživatelů do databáze RADIUS serveru. Řešení jako předchozí nabízené vyžaduje nákup dedikovaného zařízení pro RADIUS server a úplné přepracování stávající sítě.

5 Zhodnocení výsledků

Na základě předešlých analýz a preferencí společnosti, si firma kladla požadavek na dostatečné zabezpečení firemní sítě za přijatelnou cenovou hladinu, která nenaruší stávající rozpočet.

Jako rychlé a efektivní řešení současného stavu zabezpečení bylo firmě doporučeno použít kombinaci zabezpečení pomocí filtrace MAC adres, VPN, zabezpečení pomocí 802.11i a Firewallu, který je zabudován uvnitř routeru.

Výhodou nabízeného řešení je možnost kontroly připojených zařízení, jež by byla přidána do filtru MAC adres. Jelikož se jedná o poměrně malou společnost, kde by případný pokus o neautorizované přihlášení na router byl rychle odhalen a zneškodněn. Nevýhodou řešení pomocí filtrace MAC adres je, že může dojít k odcizení zařízení a než bude MAC adresa zařízení přidána do seznamu zakázaných zařízení pro přístup do vnitřní sítě, může útočník síť napadnout.

Nabízené řešení zahrnuje zabezpečení pomocí VPN, řešení má výhodu v zašifrovaném tunelu, přes který bude veškerá komunikace mezi klientem a VPN serverem probíhat, například pokud uživatel bude řešit nějaké problémy vzdáleně z domova, nebude se muset obávat, že odeslaná a přijatá data budou možný útočníkem odposlechnuta. Nevýhodou řešení však je, že pokud VPN server nebude dostupný, veškerá komunikace, která probíhala tímto tunelem, bude ukončena.

Společnost již z vlastní iniciativy na zabezpečení nastavila na routeru z původního zabezpečení WPA na zabezpečení 802.11i, které pracuje na bázi silného šifrování AES, výhodou 802.11i oproti WPA je lepší šifrování probíhající komunikace.

Firmě bylo doporučeno, aby nastavila na Firewallu URL filtr znemožňující přístup uživatelům na nevhodné stránky, které mohou podporovat rasismus, sexuální kontext, nebo jiné stránky, jenž nejsou spjaté s náplní práce. Filtr síťových služeb nebyl společnosti nastaven.

Podniku bylo navrženo, aby zvážil antivirovou ochranu pro odvrácení možných dalších útoků a hrozeb.

Pro současný stav společnosti, která se řadí mezi tak zvané „rodinné firmy“, je navrhované řešení z ekonomického a bezpečnostního hlediska jediné optimální.

Z pohledu možného budoucího rozvoje firmy bylo společnosti doporučeno nadále využívat navržené řešení, avšak s tím rozdílem, že by měla do svého řešení zahrnout také RADIUS server.

Řešení pomocí RADIUS serveru by bylo vhodné pro firmu z důvodu nutné autentizace uživatelů, kteří by se snažili připojit do vnitřní sítě pomocí přístupových bodů v rámci společnosti. Kdykoliv by se neoprávněný uživatel pokoušel připojit k takto spravovaným přístupovým bodům, uživatel by obdržel hlášku „přístup odepřen“, kvůli neuvedenému záznamu v databázi RADIUS serveru. Nevýhodou řešení je, že nezajišťuje již další zabezpečení, proto je potřeba, aby RADIUS server byl doprovázen dalšími typy zabezpečení.

Firma si zabezpečení sítě pomocí RADIUS serveru nepřeje v blízké době zahrnout do své infrastruktury, z důvodu velkých nákladů na pořízení dedikovaného serveru a nutného zásahu do firemní sítě.

6 Závěr

Při psaní bakalářské práce jsem si osvojil nové poznatky a postřehy z oblasti zabezpečení bezdrátových sítí. Poznatky a postřehy byly zahrnuty do praktické části bakalářské práce, která mapuje možná zabezpečení firemní sítě a jejich následnou implementaci do podnikové infrastruktury.

Řešení byla mezi sebou porovnána jak z hlediska nutnosti přepracování firemní sítě, bezpečnostních hledisek, která jednotlivá řešení nabízejí, tak i z hlediska finančního. Firma v současném stavu preferuje více finanční hlediska než bezpečnostní.

Pro současný stav zabezpečení byla společnosti doporučena kombinace zabezpečení pomocí MAC adres a VPN, díky nízkým nákladům na realizaci a malému počtu zásahů do stávající firemní sítě.

Můj osobní názor je, že firma by měla spíše upřednostňovat hledisko bezpečnostní před finančním, protože firma pracuje a bude pracovat i nadále s citlivými daty klientů, která může případný útočník zneužít ve svůj prospěch. Z toho vyplývá, že na bezpečnosti vnitřní sítě se nevyplácí šetřit, avšak cena řešení je také rozhodujícím faktorem, jenž si musí společnost definovat již při začátku podnikání. Hlavními otázkami zabezpečení je, co se bude v rámci firmy řešit, jaká data se budou pohybovat uvnitř společnosti a kam informace budou směřovat. Na základě těchto kritérií je třeba rozhodnout, kterému z hlavních aspektů bude dána přednost.

Bakalářská práce může sloužit jako podklad pro budoucí diplomovou práci, jež by mohla rozebrat do podrobnějších detailů a následně zpracovat kompletní navržení zabezpečení firemní sítě.

7 Použitá literatura a zdroje

1. DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. 80-251-0106-1.
2. SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Brno: Computer Press, 2010. 978-80-251-3363-7.
3. DOSTÁLEK, Libor a Alena KABELOVÁ. Velký průvodce protokoly TCP/IP a systémem DNS. Praha: Computer Press, 2000. 80-7226-323-4.
4. PUŽMANOVÁ, Rita. Širokopásmový Internet: přístupové a domácí sítě. Brno: Computer Press, 2004. 80-251-0139-8.
5. —. Bezpečnost bezdrátové komunikace: jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G. Brno: CP Books, 2005. 80-251-0791-4.
6. BARKEN, Lee. Wi-Fi: jak zabezpečit bezdrátovou síť. Brno: Computer Press, 2004. 80-251-0346-3.
7. KYSELA, Jiří. Bezdrátový Internet a technologie Wi-Fi v České republice. 2010. Dostupné z WWW:

http://www.internetprovsechny.cz/bezdratovy-internet-a-technologie-wi-fi-v-ceske-republice/

8. PITZAK, Clint. Security Analysis on WEP. [Online]. Dostupné z WWW:

http://www.eeprojects.com/wep.html

9. CTU.CZ. Český telekomunikační úřad. [Online]. Dostupné z WWW:

http://www.ctu.cz

10. PCWORLD.CZ. Internet, krátce o historii Wi-Fi. [Online]. Dostupné z WWW:

http://pcworld.cz/internet/kratce-o-historii-technologie-wi-fi-45926

11. Vacovský, Marek. Cesta do historie Wi-Fi sítí. 24/04/2013. [cit. 16/09/2015]. Dostupné z WWW:

http://mobilenet.cz/clanky/cesta-do-historie-bezdratovych-wi-fi-siti-26002

12. LUPA. CZ. Server o českém Internetu. [Online]. Dostupné z WWW:

http://www.lupa.cz

13. WI-FI.UNAS.CZ. IEEE 802.11. [Online]. Dostupné z WWW:

http://wi-fi.unas.cz/ieee-802-11.php

14. EPRIN.CZ. Základní přehled standardů IEEE 802.11.[Online]. Dostupné z WWW:

http://www.eprin.cz/

15. Košťál, Ondřej. WiFi v roce 2015: Standard 802.11ad na frekvenci 60 GHz s až 5 Gbit/s. 24/02/2014. [cit. 29/09/2015] Dostupné z WWW:
http://pctuning.tyden.cz/index.php?option=com_content&view=article&id=29244&catid=1&Itemid=57
16. EARCHIV.CZ. Archiv článků a přednášek Jiřího Peterky. [Online]. Dostupné z WWW:
http://earchiv.cz/
17. SVETSITI.CZ. Informace ze světa počítačových sítí. [Online]. Dostupné z WWW:
http://www.svetsiti.cz/
18. HOWTOGEEK.COM. [Online]. Dostupné z WWW:
http://www.howtogeek.com/
19. WIFT. Co to je DDoS útok a jak se dělá? 24/01/2012. [cit. 18/10/2015]. Dostupné z WWW:
http://diit.cz/clanek/co-to-je-ddos-utok-a-jak-se-dela
20. Pužmanová, Rita. Bezpečnost WiFi záleží jen na vás. 01/11/2007 [cit. 30/11/2015]. Dostupné z WWW:
http://www.lupa.cz/clanky/bezpecnost-wifi-zalezi-jen-na-vas/
21. Scheras. Symetrické a asymetrické šifrování. 23/10/2013. [cit. 19/11/2015]. Dostupné z WWW:
http://www.soom.cz/clanky/1126--Symetricke-a-asymetricke-sifrovani
22. BEZDRATOVESITE.WZ.CZ. Bezdrátové sítě. [Online]. Dostupné z WWW:
http://bezdratovesite.wz.cz/
23. Přibyl, Tomáš. Hříchy a zabezpečení bezdrátových sítí.[cit. 29/11/2015]. Dostupné z WWW:
http://www.ictsecurity.cz/odborne-lanky/hichy-zabezpeeni-bezdratovych-siti.html
24. Lehembre, Guillaume. Bezpečnost Wi-Fi – WEP, WPA a WPA2. 01/2006. [cit. 30/11/2015]. Dostupné z WWW:
http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_CZ.pdf
25. MartasW. Jak zjistit MAC adresu počítače. 11/02/2014 [cit. 20/12/2015]. Dostupné z WWW:
http://martasw.9e.cz/svet_it/mac_adresa_pc

26. Alan Henry. Why You Should Start Using a VPN (and How to Choose the Best One for Your Needs). 05/09/2012 [cit. 30/12/2015]. Dostupné z WWW: http://lifehacker.com/5940565/why-you-should-start-using-a-vpn-and-how-to-choose-the-best-one-for-your-needs
27. Andrew Tarantola. VPNs: What They Do, How They Work, and Why You're Dumb for Not Using One. 26/03/2013 [cit. 07/01/2016]. Dostupné z WWW: http://gizmodo.com/5990192/vpns-what-they-do-how-they-work-and-why-youre-dumb-for-not-using-one
28. Tracey Wilson. Securing Networks: Access Control List (ACL) Concepts. [cit. 17/01/2016]. Dostupné z WWW: https://www.pluralsight.com/blog/it-ops/access-control-list-concepts
29. Samuraj. Cisco IOS 8 - ACL - Access Control List. 20/07/2011 [cit.25/01/2016]. Dostupné z WWW: http://www.security-portal.cz/clanky/cisco-ios-8-acl-access-control-list
30. VPNLIST.CZ. [Online]. [cit. 10/02/2016]. Dostupné z WWW: http://www.vpnlist.cz/index.html
31. CYBERGHOST.COM. [Online]. [cit. 18/02/2016]. Dostupné z WWW: http://www.cyberghostvpn.com/en
32. IPVANISH.COM. [Online]. [cit. 18/02/2016]. Dostupné z WWW: https://www.ipvanish.com/support.php
33. TORGUARD.COM. [Online]. [cit. 18/02/2016]. Dostupné z WWW: https://torguard.net/anonymoustorrentvpn.php
34. HOW A RADIUS SERVER WORKS.COM. [Online]. [cit. 21/02/2016]. Dostupné z WWW: http://networkradius.com/how-a-radius-server-works/index.html
35. Tomáš Huňka. Technologie počítačových sítí RADIUS. 10/01/2015. [cit. 21/02/2016]. Dostupné z WWW: http://www.cs.vsb.cz/grygarek/TPS/projekty/0405Z/RADIUS/index.html#2. RADIUS
36. CISCO. COM. [Online]. [cit. 21/02/2016]. Dostupné z WWW: http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html