UNIVERZITA PALACKÉHO V OLOMOUCI

PEDAGOGICKÁ FAKULTA

Katedra technické a informační výchovy

Bakalářská práce

Lukáš Kohout

Problematika zabezpečení školní počítačové sítě

Olomouc 2016 **Vedoucí práce: Doc. PhDr. MIROSLAV CHRÁSKA, Ph.D.**

Prohlášení

Prohlašuji, že jsem bakalářskou práci na téma Problematika zabezpečení školních počítačových sítí zpracoval samostatně a použil jsem pouze zdroje, které cituji a uvádím v seznamu použité literatury.

V Prostějově 19. 4. 2016 Lukáš Kohout

Poděkování

Děkuji Doc. PhDr. Miroslavu Chráskovi, Ph.D. za odborné vedení bakalářské práce, poskytování rad a podkladů k vypracování práce. Také bych chtěl poděkovat správcům sítí za poskytnutí rad i osobních zkušeností se správou.

Obsah

Úvod

Počítače jsou dnes využívány ve všech oblastech lidského života, ať již v pracovních nebo soukromých. Mnohdy si ani uživatelé neuvědomují, že používají počítač, ani že je tento počítač právě připojen do nějaké sítě. Dnes už je velká většina všech počítačů propojena různými druhy sítí. V poslední době se nutnost připojení počítačů k síti stále více zdůrazňuje a je vyžadována pro fungování různých zařízení.

Počítačové sítě vznikly pro umožnění komunikace mezi počítači, propojení a sdílení prostředků. Jsou dnes prakticky základem jakéhokoliv podniku a jejich využívání je stále častější. Stejně tak se děje i ve školách, kde se do těchto sítí připojují školní zařízení k podpoře výuky, elektronická zařízení učitelů i zařízení studentů. A stejně jako ve společnostech i ve školách jsou tato zařízení užívána stále častěji a k stále širšímu spektru úloh. To vede k usnadnění a urychlení práce. Tyto výhody s sebou však nesou i nemalá rizika.

Prakticky každý den se dozvídáme o útoku na počítačové sítě organizací společností působících na Internetu. I my jako uživatelé se těchto útoků můžeme nevědomky účastnit. Ať jde o šíření virů, nevyžádaných e-mailů nebo o cílené útoky, vždy se jedná o problém, jehož neřešení může mít závažné důsledky. Bezpečnost síťového provozu by měla být prioritou každé organizace a podniku. K zabezpečení počítačové sítě je nezbytné splnit několik podmínek: pochopit fungování počítačových sítí a přesvědčit či donutit uživatele, kteří budou v této počítačové síti pracovat, o nutnosti konat podle daných bezpečnostních pravidel.

Toto téma bakalářské práce jsem si zvolil právě z toho důvodu, že při spolupráci na praktické realizaci různých sítí jsem se osobně přesvědčil o neznalosti a někdy i naivitě uživatelů, kteří jsou naváděni reklamami k užívání služeb bez toho, aniž by tušili, co se na pozadí děje. Z toho vyplývá pro projektanty a správce sítě nutnost zabezpečení sítí, aby byli schopni zajistit jejich provoz a ochranu.

Cíl práce

Hlavním cílem bakalářské práce je přiblížení problematiky bezpečnosti počítačových sítí na školách.

Cílem teoretické části je shrnout technické prostředky pro budování sítí. Definovat školní počítačovou síť a zjistit, jak moc se liší školní síť od podnikové. Popsat typické struktury sítě a obvyklé způsoby využívání výpočetní techniky ve školách, jejich typické uživatele a problémy. Shrnout využívanou výpočetní techniku ve školách. Doplnit možnosti a důvody využití VPN. Popsat možnosti zabezpečení sítě i bezpečného přístupu do ní. Přiblížit bezdrátovou komunikaci a její možnosti zabezpečení, typy autentizace uživatelů a počítačů připojovaných do sítě. Charakterizovat nejčastější problémy a užívané útoky na počítačové sítě. Nakonec shrnout doporučení odborníků pro bezpečnou správu sítě.

Cílem praktické části je popsat sítě budované ve školách a specifikovat přitom použité prostředky a užitá zabezpečení. Síť jako celek zhodnotit, poukázat na slabiny a chyby v návrhu a provozu. Na základě teoretické části navrhnout možná zlepšení provozních vlastností a zabezpečení sítě před zneužitím. Z nasbíraných poznatků a zkušeností správců počítačových sítí navrhnu modelový příklad, jak budovat školní počítačovou síť. Jak využít strukturu sítě jako základ jejího zabezpečení, které bude pokračovat zabezpečením aktivních prvků sítě.

1 Definice školní počítačové sítě

Počítačové sítě jsou s námi už nějaký čas. Pronikly už do všech odvětví lidské činnosti a jejich význam narůstá doslova každým dnem. Jak vlastně můžeme definovat počítačovou síť? Co vlastně pojí školu s počítačovými sítěmi? Liší se v něčem od sítí firem? Na tyto a další otázky se zaměřuje tato kapitola. V této bakalářské práci předpokládám určitou znalost problematiky na straně čtenáře. I tak myslím, že je na místě krátké přiblížení zařízení a pojmů, které se v školní počítačové síti vyskytují.

1.1 Počítačová síť

Pojmem počítačová síť chápeme spojení dvou a více počítačů tak, aby mohly realizovat výměnu informací. Umožňuje tak uživateli podle jistých pravidel komunikaci za účelem sdílení softwarových a hardwarových zdrojů (ManagementMania.com, 2011).

1.2 Vznik a vývoj počítačových sítí

K vytvoření první počítačové sítě došlo 2. září 1969 (Roubal, 2010). Tento pokus nesl název Arpanet, pojmenované podle americké Agentury ministerstva obrany. Během podzimu se takto spojily čtyři americké univerzity.

K dalšímu velkému pokroku došlo v roce 1973. V tomto roce byl přestaven protokol TCP/IP (Roubal, 2010). Od tohoto okamžiku se hovoří o Internetu v tom smyslu, jak ho známe a dnes používáme. V roce 1983 se Arpanet dělí na dvě sítě – jedna pro vojenské využití, z druhé vzniká internet v dnešní podobě.

1.3 Rozdělení počítačové sítě

Na sítě se lze dívat z podle různých hledisek. Dělíme je podle přepojování, druhu signálů, uživatele, rozlehlosti. Pro nás jsou důležité v této práci důležité rozdělení z hlediska velikosti, a proto se jí budeme věnovat obšírněji.

1.3.1 Dělení podle rozlehlosti sítě

Podle velikosti a účelu rozlišujeme sítě na čtyři základní skupiny (Roubal, 2010):

- **PAN** (Personal Area Network) – Osobní síť je velice malá počítačová síť, je to síť používaná pro propojení osobních elektronických zařízení laptop, mobil atd. Příkladem tyto sítě jsou realizovány pomocí technologií Wi-Fi, Bluetooth, Infraport (SvětHardware, 2005).

- **LAN** (Local Area Network) – Lokální počítačová síť, někdy též označovaná jako místní síť, je síť spojující uzly v rámci jedné budovy nebo několika blízkých budov typu počítač, tiskárna, server. Připojená zařízení pracují v režimu bez navazování spojení, sdílí jeden přenosový prostředek (drát, radiové vlny), ke kterému je umožněn mnohonásobný přístup (SvětHardware, 2005).

- **MAN** (Metropolitan Area Network) – „*Síť, která spojuje jednotlivé LAN, ale nepřekračuje hranice města či metropolitní oblasti, se označuje jako metropolitní síť - MAN. V rámci MAN se často používá bezdrátové spojení nebo optická vlákna. MAN může být vlastněna jednou organizací, ale většinou se jedná o propojení několika nezávislých objektů. Můžeme mít například několik poboček firmy v jednom městě propojených do MAN sítě. Dříve se využívalo technologií jako ATM a FDDI, ale dnes jsou většinově nahrazovány ethernetem označovaným jako metro-ethernet* (Boušek 2007, s. neuvedena).*“*
- **WAN** (World Area Network) - Boušek (2007) tuto síť definuje takto: „*WAN je komunikační síť, která pokrývá rozsáhlé území, jako je spojení zemí či kontinentů. Obecně můžeme říct, že jednotlivé LAN sítě se propojují přes WAN síť, aby se zajistila komunikace na velké vzdálenosti. Tímto způsobem pracuje internet jako nejrozsáhlejší a nejznámější WAN. Nejvíce se dnes asi používá technologie Frame relay případně ATM.“*

1.4 Architektury počítačových sítí

Síťová architektura je návrh komunikační sítě. Komunikace v počítačových sítích probíhá v několika fázích. Jde o otevření přenosu, přenos dat a ukončení přenosu. Na základě těchto fází lze rozdělit úlohy rozdělit do vrstev (Owebu, 2006).

1.4.1 Architektura OSI

Referenční model ISO/OSI byl vyvinut institucí International Standards Organization (Jelínek, 2005). Model dává ucelenou představu o tom, jak by počítačové sítě měly být koncipovány a řešeny. Je tvořen sérií standardů, které definují pravidla pro propojování systémů. Referenční se skládá ze sedmi vrstev, kde je každá vymezena svou funkcí. Čtyři nejnižší vrstvy jsou zaměřeny na přenos dat. Vrchní tři vrstvy jsou orientované na podporu koncových aplikací.

1.4.2 Architektura TCP/IP

Rodina protokolů TCP/IP (anglicky *Transmission Control Protocol/Internet Protocol* – protokol síťové vrstvy) obsahuje sadu protokolů pro komunikaci v počítačové síti a je hlavním protokolem celosvětové sítě Internet (SvětHardware, 2005). Komunikační protokol je množina pravidel, která určují syntaxi a význam jednotlivých zpráv při komunikaci.

1.5 Síťová zařízení

Pojmem síťové zařízení se označují všechna zařízení (prvky) připojené do počítačové sítě, které přijímají a vysílají data. Lze je rozdělit na aktivní a pasivní (Roubal, 2010).

1.5.1 Aktivní síťové prvky

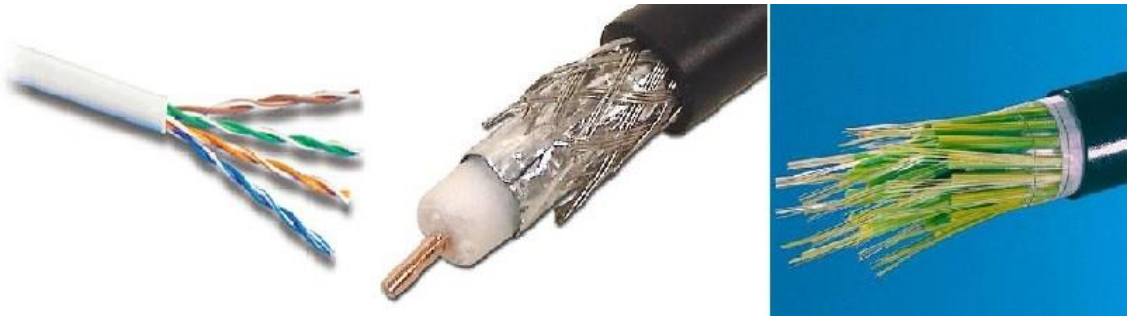
Jejich hlavní cíle je převod informací z fyzického média a následné zaslání této informace prostřednictví fyzického média k cíli. Velmi zjednodušeně se tedy dá říci, že aktivní prvky zajišťují logiku posílání dat z jednoho místa do druhého co největší rychlostí a co nejefektivnějším způsobem. Aktivní prvky zajišťují tedy činnost, která je pro konečného uživatele relativně skrytá, ale pro nejrůznější aplikace velmi důležitá právě z hlediska rychlosti, spolehlivosti a efektivitě přenosu (Roubal, 2010).

- **Hub** (rozbočovač) - je aktivní síťový prvek umožňující větvení sítě (SvětHardware, 2005). Je základem sítě topologie hvězda. Tento prvek se chová jako opakovač, což v praxi znamená, že data, která přijdou na jeden z portů, zkopíruje na porty ostatní. U této úlohy se hub nezajímá, kterému data náleží. To znamená, že všechny počítače sdílejí všechna síťová data.
- **Bridge** (most) - je síťové zařízení, které propojuje dvě části sítě na druhé (linkové vrstvě) modelu ISO/OSI (SvětHardware, 2005). Most odděluje provoz dvou segmentů sítě a zmenšuje tím tak zatížení sítě.
- **Switch** (přepínač) - Prvek počítačové sítě, který propojuje jednotlivé prvky do hvězdicové topologie (Roubal, 2010). Switch obsahuje větší nebo menší počet síťových portů na něž se připojují další části sítě. Na rozdíl od hubu však switch přeposílá síťový provoz jenom do těch směrů, do kterých je potřeba.
- **Router** (směrovač) - Jde o síťové zařízení, které procesem označovaným routování, směruje datagramy k jejich cíli (SvětHardware, 2005). Routování probíhá na třetí vrstvě modelu ISO/OSI. Oproti switchi, jenž spojuje počítače v místní síti, router spojuje dvě sítě a přenáší mezi nimi data.

1.5.2 Pasivní síťové prvky

Pasivní síťové prvky jsou nezbytnou součástí každé počítačové sítě. Slouží k přenosu informace v podobě elektrického signálu (Hardware počítačových sítí, 2012). Data ale žádným způsobem nemění ani neovlivní.

- **Kroucená dvojlinka –** je tvořena páry vodičů, které jsou po své délce pravidelným způsobem zkrouceny a následně jsou do sebe zakrouceny i výsledné páry. Kroucená dvojlinka patří mezi tzv. symetrická vedení. Signál přenášený po kroucené dvojlince je vyjádřen rozdílem potenciálů obou vodičů.
- **Koaxiální kabel -** je souosý elektrický kabel s jedním válcovým vnějším vodičem a jedním drátovým nebo trubkovým vodičem vnitřním. Tyto vrstvy jsou odděleny nevodivou vrstvou.
- **Optické vlákno -** je skleněné nebo plastové vlákno, které prostřednictvím světla přenáší signály ve směru své podélné osy. Vlákna se používají místo kovových vodičů, protože signály jsou přenášeny s menší ztrátou a zároveň jsou vlákna imunní vůči elektromagnetickému rušení.



Obrázek 1 Typy datových kabelů (převzato z www.samuraj-cz.com, 2007)

1.6 Topologie sítí

Topologie sítí (Satrapa, 2008) se zabývá zapojením různých prvků do počítačových sítí a zachycením jejich skutečné (reálné) a logické (virtuální) podoby (datové linky, síťové uzly). Jako taková je součástí teorie grafů a zasahuje tedy i do matematiky.

Topologii lze uvažovat jako určitý tvar či strukturu dané sítě. Takovýto tvar nemusí nutně korespondovat se skutečným tvarem sítě. Jde však o tvar logický. Na topologie lze nahlížet ze dvou hledisek.

- **Fyzická topologie -** popisuje reálnou konstrukci sítě, jednotlivé uzly a fyzicky zapojená zařízení a jejich umístění.

- **Logická topologie -** se vztahuje k tomu, jak jsou data v síti přenášena a kudy protékají z jednoho zařízení do druhého.

Satrapa (2008) je také dělí na základě tvaru:

Dvoubodové spoje

- **Kruh** Označuje logické zapojení, při němž je každý uzel spojen se dvěma dalšími tak, aby společně vytvořily kruh. Přenos dat je relativně jednoduchý. Výhodou je, že nevznikají kolize a náklady jsou nižší než např. u hvězdicové topologie.
- **Hvězda** Nejpoužívanější způsob propojování počítačů do počítačové sítě. Každý počítač je připojený pomocí kabelu k centrálnímu prvku - hubu nebo switchi. Mezi každými dvěma stanicemi existuje vždy jen jedna cesta.
- **Strom** Často využívaná v rozsáhlejších počítačových sítích. Vychází z hvězdicové topologie spojením aktivních síťových prvků, které jsou v centrech jednotlivých hvězd. V případě, že selže jeden síťový prvek, výpadek ovlivní pouze část sítě pod něj spadající.

Sdílené spoje

- **Sběrnice** Spojení zprostředkovává jediné přenosové médium (sběrnice), ke kterému jsou připojeny všechny uzly sítě. Má nízké pořizovací náklady, ale omezenou rychlost přenosu a také v ní může docházet ke kolizím.
- **S centrálním vysílačem.**

1.7 Školní počítačová síť

Školní počítačová síť je síť středního až velkého rozsahu. Budeme-li se bavit o školních sítích, uvažujeme velkou množinu aktivních a pasivních síťových prvků. Do školní sítě zahrnujeme počítačové učebny, jenž jsou obvykle připojeny přes ethernet. Síť bývá zavedena i pro vyučující do jejich kabinetů. Zde bývá tato síť zavedena jak přes kabel tak i bezdrátově. V současné době dochází na školách k digitalizaci školních učeben. V poslední době školy reagují na rozvoj tzv. chytrých zařízení (mobily, tablety) a začaly žákům poskytovat přístup do její sítě a k internetu. Pro výuku školy zřizují školní emaily, úložné prostory pro data a servery, na které tyto služby poskytují a řídí. Oproti podnikovým sítím, které řadíme velikostně do stejných kategorií sítí, se ve škole objevuje daleko

variabilnější množina koncových zařízení. Žáci, využívající tato zařízení, nemusí mít praktické dovednosti a mohou svým konáním ohrozit bezpečnost a provoz sítě.

2 Základní technologické charakteristiky Wi-Fi sítí

Bezdrátové sítě jsou dlouhodobě na vzestupu, protože poskytují velkou míru svobody, komfortu vyplývající z nezávislosti na fyzické kabeláži. První bezdrátové sítě byly poměrně finančně náročné a pomalé. Od té doby však technologie v této oblasti pokročila a většina společností i jednotlivců objevila pozitiva této technologie. Ke každé bezdrátové síti musí mít provozovatel od státu patřičnou licenci pro vysílání v určité frekvenci, tzv. licencované pásmo (Čížek, 2014). Původně bylo Wi-Fi alternativou pro bezdrátové připojení notebooku k síti využívající radiové spektrum, za které se nemusí platit. V současné době se Wi-Fi nadále vyvíjí. Roste jeho rychlost, bezpečnost i využití. Stále více je tato technologie využívána ve školách jak pro její zaměstnance, tak pro žáky. Proto se v této části budu zabývat charakteristikou Wi-Fi sítě. Nadefinuji pojem Wi-Fi a standard 802.11, WLAN. Představím režimy WLAN sítí jako ad-hoc sítě a infrastrukturní sítě. Své jisté místo získaly ve školních počítačových sítích.

2.1 Definice Wi-Fi

Wi-Fi (Řehák, 2003) je v informatice označení pro lokální bezdrátové sítě a vychází ze standardu IEEE 802.11. Samotný název vytvořila WECA (Wireless Ethernet Compatibility Alliance). V principu jde o bezdrátovou technologii v bezlicenčním nekoordinovaných pásmech 2,4 GHz 5 GHz. Hlavní výhodou této technologie je její nízká cena, což je způsobeno mimo jiné tím, že certifikovaná zařízení jsou k dispozici ve velkých sériích.

Standardy Wi-Fi

	rok	frekvence	teoretická rychlost
802.11b	1999	2,4 GHz	11 Mb/s
802.11g	2003	2,4 GHz	54 Mb/s
802.11a	2009	5 GHz	54 Mb/s
802.11n	2009	2,4 (5) GHz	300 (600) MB/s
802.11ac	2013	5 GHz	1 300 Mb/s

Obrázek 2 Standardy Wi-Fi (převzato z www.cnews.cz/hardware, 2014)

Většina Wi-Fi funguje na buňkovém principu (Řehák, 2003). Centrální bod zprostředkovává připojení všem stanicím v dosahu a body dohromady tvoří jakousi plástev. Propojení těchto přístupových bodů můžeme řešit různými způsoby: po lokální kabelové síti, optickým vláknem nebo přenášet i sdílená data vzduchem.

2.2 Struktura bezdrátových sítí

Bezdrátovou síť lze vybudovat různými způsoby v závislosti na žádané funkci. V rozlišení jednotlivých sítí má klíčovou roli identifikátor SSID (Thomas, 2005). Tento identifikátor je v pravidelných intervalech vysílán jako broadcast. Díky tomu si klienti mohou zobrazit dostupné bezdrátové sítě, ke kterým je možné se připojit.

2.2.1 Ad hoc sítě

WLAN sítě podle 802.11B pracují ve dvou základních režimech. První z nich je mód "ad hoc'', který je určený pro sítě typu peer-to-peer (Soom, 2008). Ad hoc režim lze použít například v situacích, kdy budujeme síť, v níž máme propojit notebook a dva stolní počítače. Vyhneme se tak instalaci kabeláže. I v porovnání s jinými typy bezdrátových sítí je její výhodou hlavně nízká cena, jelikož jedinými prvky, které je nutné instalovat, jsou bezdrátové síťové adaptéry.

2.2.2 Infrastrukturní sítě

Druhým režimem WLAN sítě je mód "infrastructure" (Soom, 2008). Tato síť obsahuje jeden nebo více přístupových bodů (Access Point), tedy zařízení, které je schopné zajišťovat komunikaci všech připojených klientů. Tyto body pravidelně vysílají své SSID. Klient si pak na základě názvu sítí vybírá, ke které se připojí. Několik přístupových bodů může mít stejný SSID identifikátor a klient se rozhoduje, ke kterému z bodu se připojí. Kritériem proto, který bod vybrat, je nejčastěji síla signálu.

3 Základní bezpečnost počítačové sítě

Počítačové sítě se staly samozřejmostí běžného života jedinců i organizací. Jejich vývojem dochází ke zrychlování komunikace. Bohužel s tím přibyly možnosti napadení sítě. Proto je nutno při budování sítě myslet na bezpečnost. Důležité je však nezapomenout na potřeby samotného uživatele. Proto je nutné při zabezpečování najít zdravý kompromis mezi bezpečností a funkčností.

Při zabezpečování je nutné definovat, jakou síť zabezpečujeme, o jak velkou síť se jedná, jaká data budeme přenášet. Na základě toho se budeme zabývat počtem implementovaných bezpečnostních vrstev. To nám řekne, kolik prostředků finančních a časových do zabezpečení investovat.

Pokud budeme definovat, co je to zabezpečení sítě, měli bychom se zaměřit na nejproblematičtější část a to jsou provozované aplikace a funkce. Zabezpečení sítě tedy je ve své podstatě minimalizace zranitelných míst síťových prostředků.

Podle Pužmanové (2005) je pro správné zabezpečení sítě nutné ochránit tyto prvky:

- Informace a data (včetně dat spojených s bezpečnostními opatřeními).
- Služby přenosu a zpracování dat.
- Zařízení.
- Uživatele (z hlediska svého majetku a identity).

3.1 Bezpečnostní politika

Autorka Pužmanová (2005, s. 15) definuje bezpečnostní politiku následujícím způsobem: „*Bezpečnostní politika je obecně založena na principu rozpoznání autorizovaného a neautorizovaného chování. Dohodnutá bezpečnostní politika se implementuje za použití různých mechanismů, které slouží k prevenci, detekci nebo nápravě. Bezpečnostní politika podnikové sítě musí podporovat cíle celého podniku, musí být jasně definovaná jako součást organizačního řízení a odpovědnosti musí být jasně deklarovány. Politiku je třeba také periodicky prověřovat, nejlépe externími zdroji. Současně musí být použité bezpečnostní prostředky i nákladově efektivní, s vědomím, že 100% zabezpečení nelze nikdy dosáhnout. Bezpečnostní politika musí být také naplnitelná a použitelná zaměstnanci, proto při její přípravě musí být brán ohled na potřeby všech podnikových oddělení.*“

Podle Pužmanové (2005) mezi bezpečnostní služby v sítích patří:

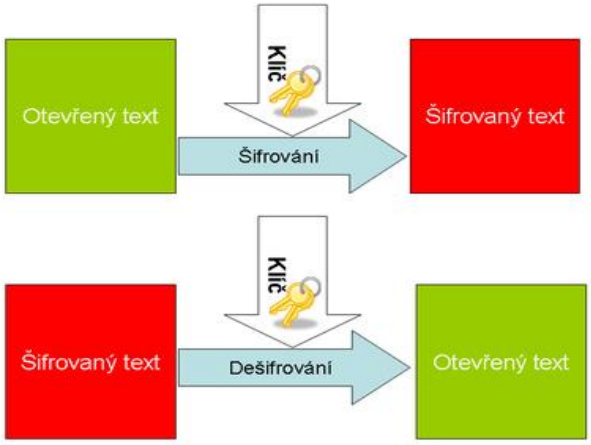
- **Autentizace** – Ověření totožnosti druhé strany, se kterou máme v úmyslu otevřít komunikační kanál.
- **Řízení přístupu** – Identifikace uživatele, umožňující přístup do systému a na jehož základě jsou přidělena práva.
- **Zajištění utajení a důvěrnosti přenášených dat** – Ochrana před neautorizovaným únikem informací, většinou řešeno šifrováním.
- **Zabezpečení integrity** – Ochrana dat před jakoukoliv modifikací, duplikací nebo zničením dat.
- **Ochrana proti odmítnutí původní zprávy** – Snaha o zabránění odesílateli nebo příjemci odmítnout potvrzení o vyslání nebo přijetí zprávy, například pomocí důkazu o původu nebo důkazu o doručení.

3.2 Šifrování

Existují dva základní přístupy k šifrování: symetricky (soukromým klíčem) a asymetricky (dvěma klíči soukromým a veřejným) – (Sosinsky, 2010). To můžeme uplatňovat na různých vrstvách síťové infrastruktury.

3.2.1 Symetrické šifrování

Symetrické šifrování (Microsoft support, 2007) je nejstarší a best-known techniku. Obě strany komunikace sdílejí stejný klíč, kterým se zpráva jak šifruje tak dešifruje. Symetrické šifrování je jednoduché a výpočetně nenáročné. Problémem je nutnost sdílení tajného klíče.



Obrázek 3 Symetrické šifrování (převzato z www.wikipedia.org, 2016)

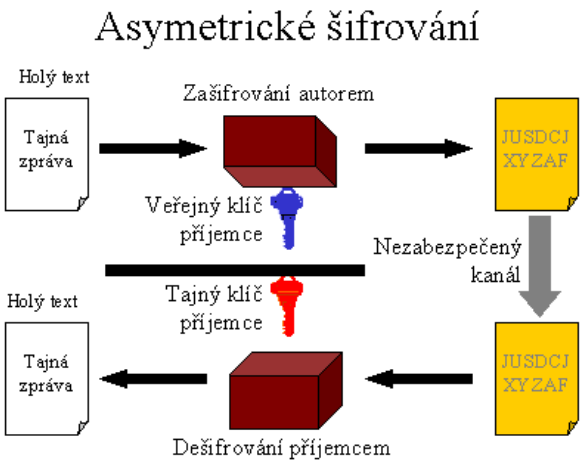
Příklady šifrování soukromým klíčem (Pužmanová, 2005):

- **DES** (Data Encryption Standard) – V současnosti se již nevyužívá. Šifrování užívá 56bitový klíč na blok o délce 64 bitů.
- **3DES** – Je vylepšením pro šifrování užívá trojité užití klíče DES.
- **AES** (Advanced Encryption Standard) - Využívá délky klíčů 128, 192, 256 bitů k šifrování bloků o délkách 128, 192, 256 bitů. Dnes se používá v rámci zabezpečení WPA2 dle standardu IEEE 802.11i

3.2.2 Asymetrické šifrování

Asymetrické šifrování (Microsoft support, 2007) ke své funkci používá pár vzájemně korespondujících souvisejících klíčů. Veřejný klíč je volně zpřístupněný všem uživatelům, kteří budou chtít posílat zprávy. Druhý soukromý klíč je udržován v tajnosti, a zná pouze majitel. Všechny zprávy (text, binární soubory nebo dokumenty), které jsou zašifrovány pomocí veřejného klíče, lze dešifrovat pomocí veřejného algoritmu, ale pouze odpovídajícím soukromým klíčem. A naopak všechny zprávy, které jsou zašifrovány pomocí soukromého klíče, lze dešifrovat pouze pomocí odpovídajícího veřejného klíče. To znamená, že se nemusíte starat o předávání veřejných klíčů v síti Internet (klíče mají být Veřejné). Problémem je, že asymetrické šifrování je pomalejší a vyžaduje více výkonu.

Pro použití asymetrického šifrování je nutné najít způsob, jak uživatelé zjistí Veřejný klíč. Typickým způsobem je distribuce použitím digitálních certifikátů.

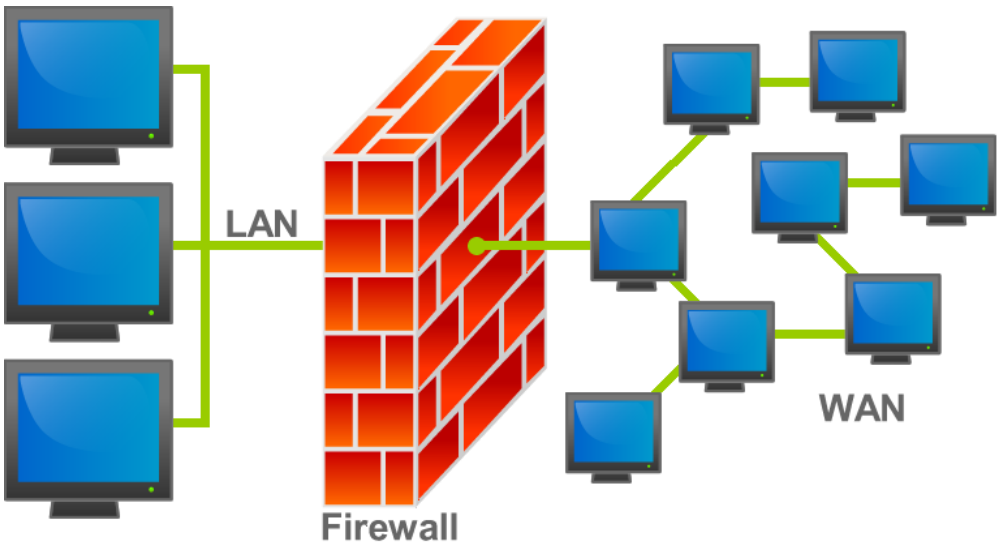


Obrázek 4 Asymetrické šifrování (převzato od sandbox.cz/~varvara/El_podpis, 2001)

3.3 Firewall

Firewall (Světhardware, 2005) je bezpečnostní brána, která definuje pravidla komunikace mezi sítěmi s různou úrovní důvěryhodnosti nebo zabezpečení a také určuje, která komunikace je povolená a která ne. Tím chrání zařízení před únikem dat nebo jiným zneužitím. Firewall kontroluje zdrojovou a cílovou IP adresu, zdrojový a cílový port, informace o stavu spojení, dále může obsahovat kontrolu protokolů, systém pro detekci útoků a další. Firewally lze zařadit do několika kategorií: paketové filtry, aplikační brány, stavové paketové filtry a stavové paketové filtry s kontrolou protokolů a IDS.

- **Softwarový firewall** je integrován v operačním systémech nebo jej můžeme stáhnout jako software z internetových stánek. Takovéto firewally jsou předem přednastaveny a mohou být poskytnuty i zdarma. Podle výzkumu (Peek, 2016) patří mezi nejlépe hodnocené Comodo Firewall, Kasperky Internet Security, ZoneAlarm. Výhodou těchto systému je větší množství funkcí.
- **Hardwarový firewall** je oproti softwarové verzi efektivnější. Hardwarová verze běží na vlastním stroji, které má pouze tento jediný účel. Kvůli tomuto oddělení je považován za bezpečnější. Zařízení vyrábí společnosti Zyxel, Cisco, Fortinet.



Obrázek 5 Firewall (převzato z www.wikipedia.org, 2015)

3.3.1 Funkce firewallu

- **Paketové filtry**

Paketový filtr je nejstarší a nejjednodušší forma firewallu (Piskač, 2008). Jeho nastavení a pravidla určují, z jaké adresy a z jakého portu může být paket přijat. Výhodou tohoto typu je rychlost zpracování. I přes svou zastaralost se používá i dnes, nejčastěji na místech, kde má procházet velké množství dat s velkou rychlostí. Nevýhodou je nízká úroveň kontroly, která se týká kontroly procházejících spojení. Tento problém je výrazný zejména u složitějších protokolů. Nejen, že nedostačuje ke kontrole vlastního spojení, ale pro takové spojení je třeba otevřít i porty, které mohou být využity jinými protokoly, než správce sítě zamýšlel.

Mezi tyto paketové filtry patří např. Access Control Lists

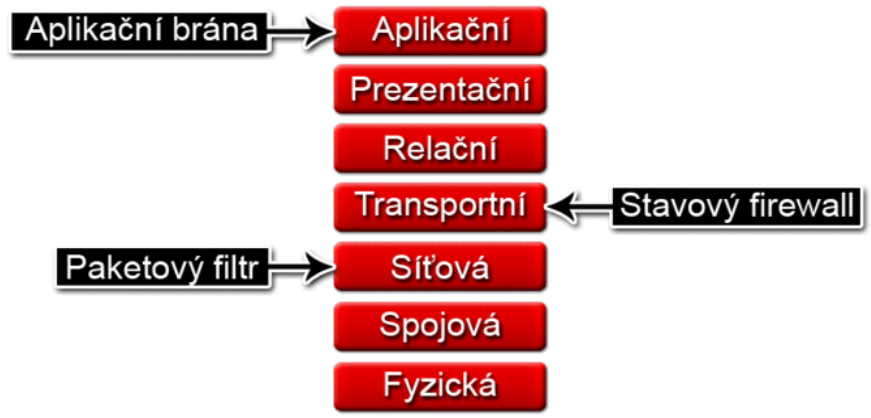
- **Aplikační Brány** (Proxy firewally)

Aplikační brána je specializovanou aplikací, která zajišťuje komunikaci internetových protokolů mezi vnitřní chráněnou sítí a vnějším světem, Internetem (Piskač, 2008). Při použití aplikační brány probíhá komunikace formou dvou spojení. Klient se nejprve připojí k proxy. Proxy toto spojení zpracuje a dále podle požadavků klienta otevře nové spojení k serveru, kde klientem je aplikační brána. Brána dostane data od serveru, které pak předá klientovi.

Jak název napovídá, kontrola probíhá na sedmé vrstvě síťového modelu OSI.

Výhodou je dobré zabezpečení známých protokolů. Kvůli své hardwarové náročnosti se používá ve velice specializovaných nasazeních.

Mezi zástupce aplikačních bran patří např. The firewall Toolkit (FWTK.ORG, 2015).



Obrázek 6 Firewally pracující na různých vrstvách OSI (převzato z www.wikipedia.org, 2014)

- **Stavové paketové filtry**

  Tyto filtry fungují stejně jako paketové filtry, ale navíc ukládají informace o spojích, které jsou povolené (Piskač, 2008). Ty se následně používají při rozhodování, zda jde o povolené spojení a může být propuštěno nebo zda musí projít procesem rozhodování. Tento systém urychluje zpracování paketů již povolených spojení. Dále lze v pravidlech pro firewall uvádět jen směr navázání spojení a ten pak bude schopen povolit i odpovědní pakety.

  Výhodou tohoto typu je vysoká rychlost, slušná úroveň zabezpečení a jednoduchá konfigurace.

  Mezi představitele patří např. FireWall.

3.4 IDS a IPS Sondy

„IDS (Intrussion Detection System) je systém, který detekuje narušení (potencionální útok) (4safety, 2011, s. neuvedena). IDS jsou centrálně orientované systémy, které se skládají ze sond detekujících útoky, databáze, do které jsou tyto záznamy ukládány a centrální management konzole, ze které je možné do databází nahlížet, ale také generovat výstupy. Tyto výstupy mají formu, kterou si stejně jako typ informací, které obsahují, může administrátor přizpůsobit. Některé tyto konzole disponují vyspělými analytickými nástroji.

Pod pojmem IPS (Intrussion Prevention systém) je pokračování IDS. Zatímco úkolem IDS je útoky detekovat, pak úkolem IPS, je útoky detekovat a zastavit. Na první pohled to vypadá, že IDS nemají na trhu již místo. Realita je ale zcela odlišná. IPS rozhodně není vhodným řešením pro každou implementaci.“ (4safety, 2011, s. neuvedena)

- **Network IDS**

Jde o systém pracující na úrovni síťové komunikace. Průchozí provoz je analyzován technologií Protokol Anomaly Detection (PAD) a při správném nastavení odhaluje nekorektní síťový provoz. To může být užitečný nástroj pro zabezpečení, bohužel tato technologie má slabiny, které mohou provoz na síti zastavit. Hlavní slabinou je, že standardy protokolu jsou vyvíjeny rychleji než případné aktualizace pro PAD. Kvůli tomu pak může být korektní provoz označován jako nekorektní a je vyhodnocen jako útok. Při analýze technologií PAD je paket otestován na přítomnost některé signatury, které vybírá z databáze používaných signatur. Tyto signatury představují otisky známých útoků.

- **Host IDS**

Tyto sondy se instalují přímo na server, kde detekují především lokální útoky, jenž není možné detekovat na síťové úrovni.

- **Hybrid IDS**

Hybridní systém, který kombinuje HostIDS i NetworkIDS a zajišťuje detekci útoků komplexně (4safety, 2011). Spojení probíhá přes centrální konzoli, a proto není nutné mít Network IDS a HostIDS od stejného výrobce.

4 Virtuální privátní sítě (VPN)

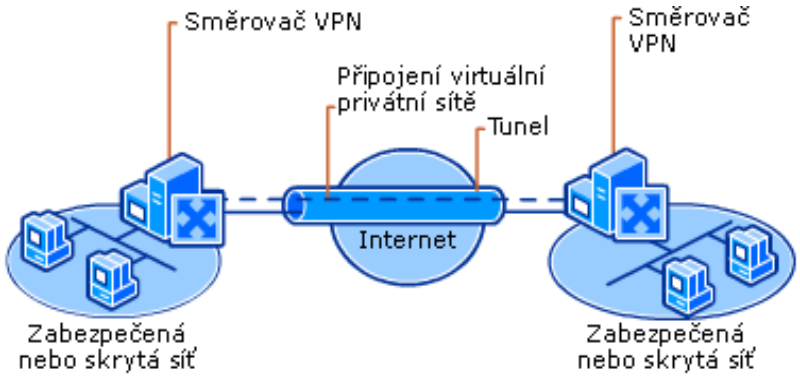
Prvořadou povinností počítačové sítě je propojení prostředků za účelem usnadnění práce a ušetření financí. S tím musíme k zabezpečování přistupovat. Nemůžeme tedy síť zabezpečit absolutně a odstřihnout ji od internetu. Potom by síť ztratila svůj význam. Proto se v této části budu věnovat tomu, jak se bezpečně připojit do vzdálené sítě. Definuji význam virtuální privátní sítě a popíši jejich funkci a fungování.

4.1 Definice

„VPN jsou propojení mezi dvěma body realizována přes veřejnou nebo privátní síť (Microsoft, 2008, s. neuvedena). Jsou zásadní pro realizaci bezpečného vzdáleného přístupu. Klient VPN pomocí speciálních protokolů založených na protokolu TCP/IP a označovaných jako protokoly tunelových propojení virtuálně volá virtuální port na serveru VPN. Při typickém nasazení sítě VPN iniciuje klient přes Internet virtuální propojení mezi dvěma body k serveru vzdáleného přístupu. Server vzdáleného přístupu přijme volání, ověří volajícího a přenese data mezi klientem VPN a privátní sítí organizace.“

4.2 Princip činnosti

Při použití technologie VPN jsou data zapouzdřena pomocí hlavičky obsahující směrovací informace, které umožňují průchod dat přes tranzitní síť (Microsoft, 2008). Přenášená data jsou z důvodu utajení šifrována. Pakety zachycené ve sdílené nebo veřejné síti nelze bez šifrovacích klíčů dešifrovat. Propojení, ve kterém jsou privátní data zapouzdřena a zašifrována, je označováno jako připojení VPN.



Obrázek 7 Propojení dvou míst přes VPN (převzato z technet.microsoft.com, 2008)

Připojení VPN pro vzdálený přístup umožňuje uživatelům pracovat se serverem v privátní síti pomocí infrastruktury veřejné sítě jako je internet (Werner, 1996). Z pohledu uživatele lze VPN chápat jako propojení mezi dvěma body, tedy mezi počítačem (klientem VPN) a serverem organizace.

VPN lze použít pro řešení různých požadavků. Tyto požadavky zahrnují bezpečnou komunikaci přes veřejnou síť a jsou tyto:

- Propojení pobočkových intranetů (site-to-site) do jedné velké podnikové sítě.
- Vzdálený přístup (remote acess) připojení vzdáleného uživatele k podnikovému intranetu.
- Extranet – vytvoření sítě vně podnikového intranetu.

4.3 VPN brány

Úkolem bran VPN je dohodnutí a poskytnutí bezpečnostních služeb (Microsoft, 2008). Brány se starají o bezpečný přístup do sítě pro oprávněné uživatele a udržení neoprávněného provozu vně sítě. Dále mají na starost šifrování komunikace mezi sítěmi a překlad NAT adres. Totožnost dvou koncových bodů, VPN brány a uživatelů, kteří posílají zprávy přes VPN, ověřuje autentizace. Pro přístup uživatele do internetu otevře VPN server port firewallu až po autentizaci.

5 Zabezpečení bezdrátové komunikace

Problém bezpečnosti Wi-Fi technologie, bez ohledu na velikost instalace, vychází z toho, že její signál se šíří i mimo zabezpečený prostor. Radiový signál se nezastaví obvodovým zdivem. Zprovoznění přístupového bodu tak může znamenat stejné nebezpečí jako instalace internetové zásuvky na veřejném místě. Útočník dokonce se dokonce nemusí k AP přiblížit. Dalším problémem této oblasti je, že bezdrátová zařízení se prodávají bez zabezpečení. Výrobci tak činí, aby jejich zařízení fungovala hned po zapnutí. Z těchto a dalších důvodů představuje bezdrátová komunikace možné bezpečnostní riziko. V této kapitole popíši možnosti, jak toto riziko co nejvíce snížit.

5.1 Omezení úniku rádiových vln

Jak bylo naznačeno v úvodu, radiovým vlnám nelze přikázat, aby se nešířily mimo hranice pozemku. Existují však opatření, která mohou míru nežádoucího uniku omezit. AP, umístěný blíže ke středu budovy, bude vně vyzařovat méně, než AP u okna. Namísto antén vyzařující na všechny strany je možné použít směrové antény a omezit vyzařování směrem dovnitř budovy. Na některých AP (Barken, 2004) je navíc možné snížit vyzařovaný výkon. Signál však musí být dostatečně silný, aby dosáhl na všechny klienty. I přes tato opatření je nutné vycházet z předpokladu, že signál lze stále zachytit i mimo budovu nepovolanými osobami.

Možnosti zabezpečení bezdrátových sítí můžeme rozdělit do dvou skupin:
Šifrování = zabezpečení přenášených dat před odposlechem
Autorizace = řízení přístupu oprávněných uživatelů

5.2 Skrytí SSID

SSID je v indikátor bezdrátové sítě (Tech-FAQ, 2012). Přístupový bod vysílá v pravidelných intervalech tento indikátor v majákovém rámci (beacon frame). Klienti si na základě tohoto indikátoru vybírají síť, ke které se připojí. Tato funkce tak zjednodušuje připojení k nějakému přístupovému bodu. To je poměrně pohodlná funkce, pokud se vyskytujete v okolí přístupového bodu. Na druhou stranu je tato funkce nepohodlná z hlediska bezpečnosti. Nechtěný klient má okamžitou možnost k nalezení a identifikování sítě. Výrobci hardware proto zavedli možnost, která se nazývá uzavřená síť.

„Smysl potlačení SSID (Barken, 2004, s. 20) spočívá v tom, že snižuje pravděpodobnost detekce sítě různými „war drivers[1]“ nebo že se k vám připojí klient jdoucí okolo.“

Jde o nejjednodušší možnost zabezpečení bezdrátové sítě tak, že zdánlivě skryjeme SSID. Klientům se tak síť nezobrazí v seznamu dostupných sítí, a to proto, že nepřijímají broadcasty s SSID. Takto lze odradit většinu nezvaných hostů. Pokud se však klient snaží připojit k přípojnému bodu, je SSID přenášeno v otevřené podobě a lze ho zachytit. Experti proto považují pouze vypnutí vysílání SSID za bezpečnostní slabinu. Měly by tak být používány i další druhy šifrování a identifikace.

5.3 Filtrace MAC adres

MAC adresa představuje jedinečný identifikátor každého zařízení obsahující síťovou kartu. Tento identifikátor, někdy nazývaný jako hardwarová adresa je přiřazována výrobcem.

Filtrace MAC adres byla vytvořena na principu, že AP si udržuje seznam autorizovaných adres, kterým je povolen provoz.

Problémem tohoto zabezpečení je, že většina bezdrátových karet umožňuje uživateli změnu této adresy a to buď přímo v operačním systému nebo pomoci aplikací jako jsou MAC Adress Changer, SMAC a další. Zdrojová a cílová adresa se posílá nešifrovaně a může dojít k tomu, že útočník může odposlechnout hodnoty povolených MAC adres. Po odposlechnutí mu pak stačí, aby změnil adresu na bezdrátové síťové kartě na platnou. AP pak novou kartu nerozpozná a bude si myslet, že jde o normální provoz.

5.4 Protokol WEP

WEP (Wired Equivalent Privacy) je označení pro starší zabezpečení bezdrátových sítí podle původního standardu IEEE 802.11 z roku 1997 (Wikipedie, 2015). To mělo poskytnout podobné zabezpečení jako má drátová počítačová síť. Protokol WEP pracuje v bezdrátové síti na linkové vrstvě a šifruje přenášené rámce pomocí proudové šifry RC4.

[1] Wardriving je prosté hledání bezdrátových sítí. Tento termín v daném kontextu jako první použil Peter Shipley, který tak chtěl poukázat na bezpečnostní rizika otevřených bezdrátových sítí.

„Algoritmus používá proudovou symetrickou šifru s délkou klíče 40, 104 a 232 bitů (Security-portal.cz, 2005, s. neuvedena). Již v roce 2001 však bylo v algoritmu objeveno hned několik bezpečnostních nedostatků. Se symetrickým šifrováním je problém v tom, že někde musí mít klient uložený statický klíč, kterým šifruje a zároveň dešifruje komunikaci. WEP bohužel nijak neřeší distribuci klíče a tak je musíme ve většině případů manuálně zapsat do konfigurace zařízení. Tím trochu odpadá podstata šifrování. Útočník sice zatím klíč nezná, ale oprávněný uživatel ano a tak pro něj není složité komunikaci dešifrovat.“

Další slabinou tohoto šifrování je prolomení klíče brutální silou, tedy při dostatečném počítačovém výkonu může útočník testováním různých klíčů najít ten správný. K tomu se dá použít program Aircrack. Podle Štraucha (2008) při použití WEP zabezpečení výpočet 128 bitového klíče trval přibližně 10 minut při napadení zevnitř sítě. Při napadení zvenku výpočet trval několik desítek minut. Podobné zkušenosti mi potvrdili přátelé studující na Přírodovědecké Fakultě.

WEP byl v srpnu 2001 prolomen, proto se od jeho používání ustoupilo a byl nahrazen protokolem WPA.

5.5 Protokol WPA

Po prolomení zabezpečení WEP, bylo v roce 2002 zavedeno zabezpečení WPA (Wi-Fi Protected Access) jako součást připravovaného standardu IEEE 802.11i (Security-portal.cz, 2010; Wikipedie, 2015).

WPA byl navržen tak, aby podporoval stávajícího vyráběný hardware, který byl zabezpečován protokolem WEP se šifrou RC4. Standardně používá 128 bitový dynamický klíč, jenž je měněn po každých 10 000 paketech. Pro odstranění slabých míst byl vyvinut protokol TKIP (Temporal Key Integrity Protokol). Ten má funkce jako dynamické regenerování klíčů, kontroly integrity zpráv a číslování paketů proti útokům.

Vadou WPA je, že i přes prodloužení klíčů a inicializačních vektorů, snížení počtu zaslaných paketů s příbuznými klíči a systému ověřujícímu integritu zpráv je dnes snadné WPA prolomit, pokud je použito společně s TKIP. Použití kombinace těchto protokolů je považováno za stejně nebezpečné jako u protokolu WEP a je doporučeno používat bezpečnější protokol WPA2.

5.6 Protokol WPA2

WPA2 implementuje všechny povinné prvky IEEE 802.11i (někdy se zabezpečení WPA2 označuje jak 802.11i) (Pužmanová, 2005). K protokolu TKIP a algoritmu Michael přibyl nový algoritmus CCMP založený na AES, který je považován za bezpečný. WPA2 certifikace je povinná na všech nových zařízeních, která chtějí být certifikována jako Wi-Fi.

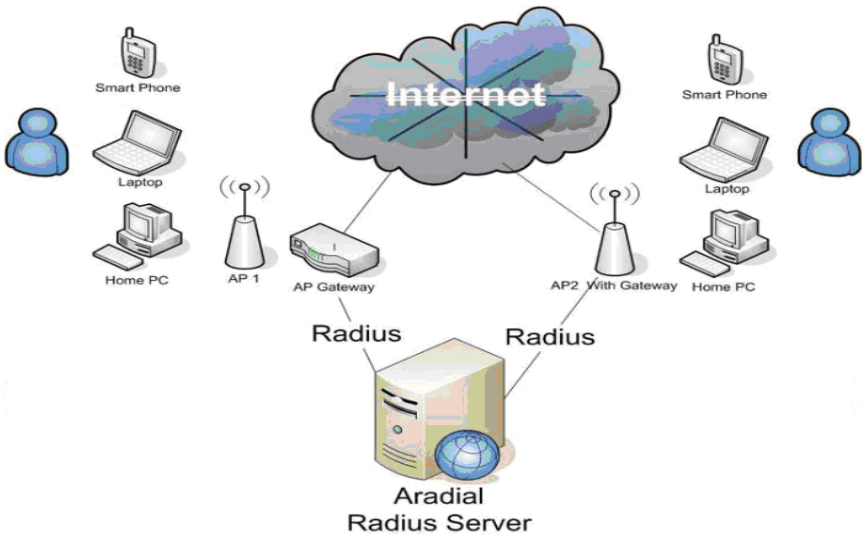
Zabezpečení WPA2 je považováno za velmi bezpečné a je proto vhodné zvolit toto zabezpečení při budování Wi-Fi sítě (Security-portal.cz, 2010).

5.7 Autentizace klienta

Pro autentizace klientů (Pužmanová, 2004) je u protokoly typu 802.11i navrženo dvojí možnost autentizace Buď použitím předsdílené fráze (tzv. PSK – Pre-shared key) anebo režim 802.1x. Úspěšnost autentizace PSK závisí na jeho uživatelích. Proto by toto heslo mělo znát jen malý počet lidí. Neméně důležitá je pak volba samotného hesla. Pokud je PSK vytvořeno na základě fráze, může být náchylné ke slovníkovým útokům. Pokud má Wi-Fi síť sdílet větší množství lidí, nabízí se řešení s použitím autentizačním serverem (např. RADIUS) pomocí protokolu IEEE 802.1x.

5.8 RADIUS

RADIUS je protokol pro přenos autentizačních, autorizačních, konfiguračních a evidenčních informací mezi přístupovým serverem (RADIUS klient) a společným autentizačním serverem (RADIUS server) (Pužmanová, 2005). Tento protokol je popsán v dokumentech RFC 2138 a RFC 2139.



Obrázek 8 Radius server (převzato od info.sks.cz, 2010)

5.9 RADIUS protokol

RADIUS pracuje v režimu klient/server, ve kterém jsou autentizační informace posílány mezi RADIUS serverem a RADIUS klientem (Havelková, 2010). Autentizační server ověří srovnáním údajů ze své databázi a identitou klienta a oznámí bezdrátovému přístupovému bodu (RADIUS klientu), zda klient je nebo není oprávněn k přístupu ke službám sítě. RADIUS klient funguje jako prostředník mezi klientem a autentizačním serverem. Autentizační server žádá identifikační informace od klienta a posílá zpět klientovi. RADIUS klient je odpovědný za zapouzdření/rozbalení Extensible Authentication Protocol (EAP) rámce a za komunikaci s autentizačním serverem. PROTOKOL je používaný z důvodu jeho vysoké síťové bezpečnosti. Ta vyplývá z toho, že transakce mezi klientem a RADIUS serverem je autentizována pomocí sdíleného tajemství, které není posíláno přes síť. Navíc jsou všechny autentizační údaje zasílány šifrovaně se sdíleným heslem symetrickým algoritmem.

5.10 Digitální certifikát

Digitální certifikát (SSL certifikát) je digitálně podepsaný klíč ve formátu X.509 (Interval.cz, 2003). Certifikát vydává certifikační autorita. Certifikát slouží k ověření identity protistrany pro navázání zabezpečené komunikace. Jeho kvalita je určena několika faktory. Certifikát lze hodnotit těmito parametry:

- Důvěryhodnost certifikační autority, která certifikát vydala.
- Kvalita použitých kryptografických algoritmů.
- Transparentnost softwarového procesu ověření certifikátu.
- Chování uživatele, který certifikát ověřuje.

Aplikace, která využívá certifikáty, nabídne postup, jak certifikát automaticky ověří. Uživatel dostane možnost ověření zkontrolovat. Každý certifikát má určitou dobu platnosti. Tento interval určuje majitel a certifikační autorita.

6 Útoky na počítačové sítě

V této části se budeme zabývat důvody, proč je nutné sítě zabezpečovat. Podíváme se na to, jakými způsoby se narušitelé dostávají do sítě.

Pužmanová (2009) rozdělila útoky na:

- **Útoky na hardware**

K útoku na hardware dochází tehdy, pokud se hacker dostane do kontaktu s počítačem k síti. Nejčastěji pak takovýto hacker provádí útok tak, že přepne síťovou kartu do promiskuitního režimu nebo že si na počítač přidá vlastní zařízení, například hardwarový keylogger. Zde se vyplatí používat šifrované spojení a investice do zabezpečení objektu. Patří sem útoky jako sniffing a keylogging a podobné.

- **Útoky na software**

Velmi často používané útoky, při kterých se využívá nedokonalosti programů či síťových protokolů k průniku do systému. Zde se podíváme na některé z nich.

6.1 Útoky na bezdrátové sítě

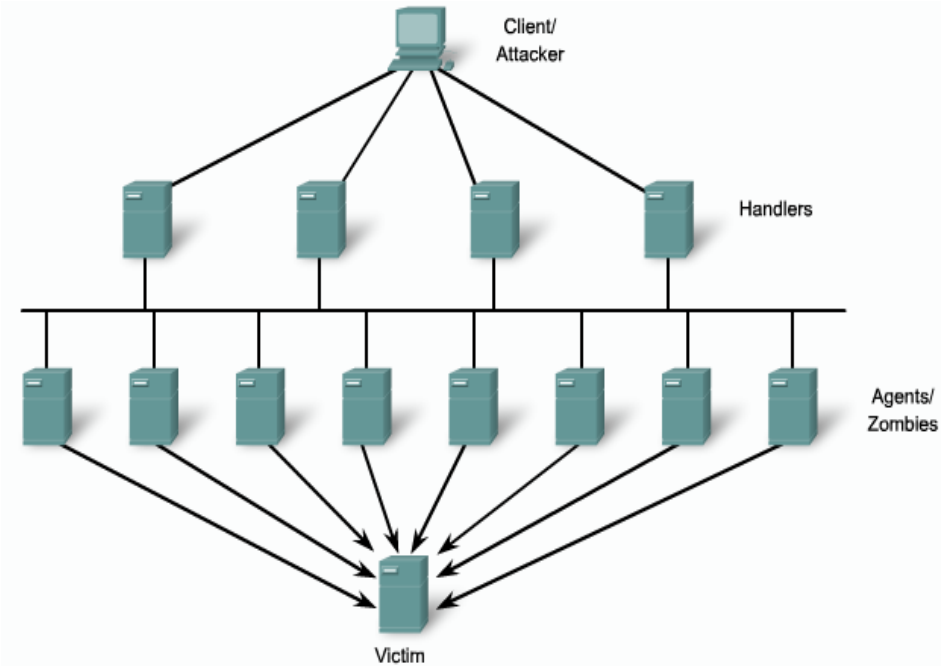
- **Falšování identity zdroje** (address spoofing) – útok prostřednictvím falešné adresace mění skutečnou zdrojovou adresu datagramu z adresy zakázané pro vstup do sítě na adresu povolenou (Pužmanová, 2009). Útočník tak dostane možnost k užívání služeb jako důvěryhodný uživatel. Dalšími dopady může být získání informací o oprávněných uživatelích a jejich účtech, přidání či změna konfigurace zařízení v síti.
- **Man-in-the-middle** (MITM) – útočník se vydává za jednu z důvěryhodných stran v konverzaci. Útočník tímto útokem zachytává zprávy přenášených v síti. (Pužmanová, 2005, s. 31) „*Útok je úspěšný, pokud se útočníkovi podaří udržet konverzaci po potřebně dlouhou dobu. Útočník musí být schopen posílat pakety a odposlouchávat odpovědi, takže buď umístí svoje zařízení na cestě mezi oprávněným uživatelem a cílovou stanicí-oběť nebo změní cestu mezi oběma komunikujícími stranami tak, aby vedla přes jeho zařízení.*“
- **Útoky na přístupová hesla** – Slabá hesla jsou dnes stále častějším problémem síťových systémů, což se přímo odvíjí od zvyšování rychlosti bezdrátové komunikace. Hesla lze odhalit různými způsoby jako falešné IP adresace, prostřednictvím programů jako jsou Trojský kůň nebo opakujícími pokusy (brutální

silou). Poslední zmiňovaný je dvojnásob nebezpečný. Opakovanými pokusy přihlásit se blokuje oprávněným uživatelů přístup ke službám.

- **Útok vedoucí k odmítnutí služby** (Dos, Denial of service) - Tento druh útoku není veden k získání přístupu do sítě, ale k znemožnění práce ostatních uživatelů na cílovém systému (Security-portal, 2013). Nejčastěji je to provedeno vyčerpáním zdrojů zařízení, nebo jejím zahlcením.
- **Útoky prostřednictvím odposlechu** – „*pro získání přenášených datagramů někde po cestě nebo vypracovanou odbočkou. Tak je možné získávat informace přímo z datagramů, měnit je nebo ničit, získávat přístup ke zdrojům sítě v rámci otevřených spojení a také analýzou datagramů odhalovat informace o vnitřní síti a jejích uživatelích.*“ (Pužmanová, 2005, s. 32)

6.2 Útoky z internetu

- **Technika DDOS -** Jde o techniku (Security-Portal.cz, 2013), pro niž je cílem odstavení poskytované služby. Tímto odstavením může být restart zařízení, jenž způsobí zastavení či přerušení poskytovaní služby. Obvyklé způsoby této techniky jsou především v přehlcení dané služby požadavky a daty. Další způsobem této techniky je umělé vytížení procesoru serveru, změna konfigurace a rušení komunikace.



Obrázek 9 Princip útoku DDoS (převzato z www.tkelement.com, 2010)

- **Technika SYN flood** (záplava) – Tato technika (Security-Portal.cz, 2013) využívá principu navazování tcp spojení mezi počítači. Toto navazování funguje tak, že klient odešle paket s příznakem SYN. Server mu odpoví paketem SYN-ACK. Klient ve třetím kroku odesílá paketem ACK. Útok se provádí tak, že klient odešle paket SYN, ale jako svou adresu uvede neexistující adresu, na kterou server odpoví, ale sám se odpovědi nedočká. Útočník svůj krok opakuje. Tímto způsobem dochází k vytvoření fronty čekajících a tu drží až do vypršení platnosti. Tato fronta má omezenou délku. Po jejím naplnění už nelze navázat nová spojení.
- **Technika UDP flood** - Útok užívá pro svou činnost User Datagram Protocol (UDP) (Špondr, 2013). Základem je zahlcení obvykle libovolně vybraného portu pakety UDP. Hostitel zkontroluje, zda nějaká aplikace vyžádala pakety a zjistí, že ne. Vygeneruje reply paket IMP o nedoručitelnosti. Při znásobení velkým počtem paketů UDP může dojít k ochromení systému.
- **Technika Ping of death** (PoD) - V současné době málo užívaný útok, dnešní systémy umí s příkazem pracovat poměrně bezpečně (Security-Portal.cz, 2013). PoD lze rozdělit na dva druhy. První varianta spočívá v zahlcení pakety. Druhý typ spočívá v umělém navýšení velikosti paketu, ve kterém dojde k odeslání příkazu ping. Ve starších systémech se pod jediným pingem zhroutila služba.
- **Technika Tear Drop** (slza) - Útok využívá logiky rozdělování velkých paketů (fragmentace) (Špondr, 2013). Pokud je paket příliš velký, odesílá se po částech tzv. fragmentech. Tyto části jsou po obdržení znovu sestaveny. Technika Tear drop posílá fragmenty, které se překrývají. To vede k tomu, že některé části dorazí dvakrát. Systém tyto fragmenty sestaví za sebe. Takto sestavený paket je však větší, než místo které si na ně systém připravil. Systém přijímající takovéto pakety se zhroutí.

6.3 Typy útoků k přístupu do systémů

Zde se budu věnovat k útokům zevnitř sítě. Tyto útoky vedou k přístupu do systému, jenž by měl vyžadovat autentizaci.

- **Útok hrubou silou** (Brutal Force Attack)

Špondr (2013) popisuje tento útok jako poměrně snadný, ale časově a zdrojově náročný typ útoku. K útoku se využívají password crackery (louskače hesel) - ty zkouší kombinace znaků jako hesla. Tyto útoky se dají optimalizovat, pokud tyto programy zkouší

hesla ze slovníku. Proto se nedoporučuje používat hesla jako „ 0000, 12345678, abcdefgh “. Takováto hesla jsou poté prolomena v jednom průchodu. Slovníkové útoky ale nezaberou, pokud je daný uživatel dostatečně chytrý a tyto hesla nepoužívá. Pak útočníkovi nezbývá než opravdový útok brutální silou. Tento útok je závislý na délce hesla. Odborníci se shodují, že zvolené heslo by mělo být minimálně 8 znaků dlouhé a mělo by v sobě kombinovat velká a malá písmena, čísla a další symboly. Tato metoda je poměrně nebezpečná pro samotného útočníka. Moderní systémy si takovéto útoky zaznamenávají do logů, protože jsou snadno vypátratelné.

- **Sociální inženýrství** (Social Engineering)

Hacker nějakým svým činem nebo chováním dostane od určitého člověka přístup k systému (Špondr, 2013). K tomu většinou dojde prostřednictvím prozrazením hesla. Jak takováto situace nastane? Velmi pravděpodobně se hacker bude ať už v reálném světě nebo na internetu vydávat za někoho, kým není. Na systém pak nainstaluje keylogger či sniffer. Uvedu zde modelovou situaci.

Osoba se připojila k určité službě a útočník započne svůj útok a odešle jednoduchý počítačový virus. Ten samotný žádnou škodu nenapáchá, zobrazí se však naší pracující osobě. Útočník pošle mailem dokument naší osobě, ve které se prezentuje jako správce sítě. Informuje naší nic netušící osobu, že na jeho účet byl veden útok a že je nutné z důvodu bezpečnosti změnit svoje přihlašovací heslo a jak tuto změnu hesla provést. Současně se do systému nainstaluje keylogger. Útočníkovi pak stačí vyčkat až keylogger zašle získané informace zpět. Další možností je hra na city či nabídka finanční odměny.

Jak se proti těmto útokům bránit? Základní obranou na počítači by měl být antivirový program. Ten by měl rozpoznat poměrně známé viry. Důležité je však chování uživatele, aby byl alespoň trochu podezíravý a podobnou událost si prověřil.

7 Doporučení pro zabezpečení sítě

V této části přiblížím základní principy a postupy, které nám pomohou síť chránit. Obrana před těmito útoky není snadná. Prvním problémem je rozlišit běžný provoz od cíleného útoku. Jak už bylo zmíněno v předchozí kapitole, většina útoků vychází z principů navržení síťových protokolů. To může na první pohled vypadat hrůzostrašně. Ve skutečnosti lze dodržovat několik pravidel.

- Při budování sítě je vhodné vybírat prostředky tak, že sám výrobce na nich nastaví alespoň základní pravidla zabezpečení.
- Útoků je celá řada a správce sítě nemá prostředky ani dostatek času hledat každou techniku útoku a hledat na ně patřičnou obranu. Prvním krokem ke zdárné ochraně sítě a zařízení je pravidelná instalace záplat vydávaných výrobcem, který má prostředky k nalezení možnosti oprav.
- Prvním obranným prostředkem v naší síti by měl být dobře nastavený firewall. Ten je pak schopný ochránit velkou množinu cílů tak, že případnému útočníkovi se nevyplatí investovat do útoku. I v případě, že se útočník snaží o útok, může dobře nastavený firewall útok zpomalit, či dokonce zastavit. V základním nastavení firewallu by měla být zakázána UDP komunikace (PCtunning, 2008).
- Změnit defaultní jména a hesla pro připojení k zařízení v síti.
- U bezdrátových sítí nastavit nejmodernější a nejsilnější zabezpečení. S tím souvisí i volba šifrovací protokolu (Pužmanová, 2009). V současnosti se používá protokol WPA2 a šifrovaní AES.
- Podle výzkumů až 70% útoků pochází od zařízení v LAN (Security-portal.cz, 2005). Proto by samozřejmostí mělo být používání aktualizovaného antiviru. Výběr prověřeného antiviru od známého výrobce může zabránit většině případných útoků.
- U velkých sítí je také možné zvážit nasazení IDS nebo IPS. Jejich spravování však vyžaduje zkušenosti. Nesprávně nastavené sondy mohou vést k nefunkčnosti sítě.
- Důležitou částí je obrana na úrovni služeb. Zakázání některých nepoužívaných služeb se zmenší množina cílů, které by mohl útočník použít k napadení sítě či jejich prvků. Zároveň tak ulehčíte samotnému serveru.
- V poslední době dochází ke stále častějšímu používání DDoS útokům. Podle serveru je obranou nastavení restrikcí na síťové úrovni (Security-portal.cz, 2013). Pro daný typ útoku je vhodná restrikce prvního paketu z nové IP adresy – útočníci obvykle

mění IP za falešnou a použijí ji vždy jen jednou. Restrikce na první použití IP tak může pokrýt velkou část útoku hned v počátku.

- V oblasti obrany serverů existují profesionální prostředky pro sledování, filtrace komunikace a blokování útoků. Tyto prostředky jsou jak hardwarové tak softwarové.
- Vypnout funkci WPS (Wi-Fi protected setup). Tato funkce má za cíl zjednodušit zabezpečení bezdrátové sítě. Je však velmi náchylná na útok hrubou silou a je proto označována za bezpečnostní riziko (Šípek, 2012).

8 Praktická část

V této části budeme popisovat zkušenosti s výstavbou, modernizací a zabezpečování dvou školních počítačových sítí, jejichž budování jsem se osobně zúčastnil v součinnosti s firmou Kohra Group s.r.o.. Při tom budeme vycházet ze zkušeností správců sítí. Při popisování výstavby jsme se zaměřili na to, jaké bylo zadání výstavby počítačové sítě, jaká byla zařízení použita. Dále se zabýváme otázkou jejich bezpečnosti. Při popisování jsme se věnovali tomu, jak je nastaven firewall, jak probíhá autentizace klientů, jak jsou řešeny přístupy do jednotlivých sítí, jaké aplikace běží v rámci sítě. Na závěr jsou tyto sítě zhodnoceny a budou k nim navržena zlepšení z hlediska jejich zabezpečení, což bude sloužit jako zpětná vazba pro správce sítí, kterým bude tato práce poskytnuta. Nakonec bude navržen model počítačové sítě.

8.1 Výstavba první sledované počítačové sítě

První popisovaná počítačová síť byla budovaná v Prostějově ve školním zařízení, jehož součástí je internátní ubytování. Pro žádost vedení zde nebude z důvodu bezpečnosti uváděno jméno.

O tuto fázi modernizace počítačové sítě se postarala firma Kohra Group s.r.o., která dál zajišťuje správu počítačové sítě. Tato firma mi poskytla informace o modernizaci sítě a jejím zabezpečení.

Požadavek tohoto projektu bylo pokrytí celého objektu Wi-Fi signálem pro ubytované klienty (žáky). Modernizace proběhla v prosinci roku 2014 a bylo zde použita moderní, ale zároveň osvědčená zařízení a prostředky:

Router - Mikrotik RB 450G použit 1x.

Switch - Zyxel GS 1910 – 24 použit 1x.

Použitá WiFi – Ubiquiti UniFI AP 2,4 Ghz použit 6x.

Další instalace - Kabel UTP CAT5e.

8.1.1 Původní stav

Při modernizaci byla využita dříve zbudovaná počítačová síť postavená na strukturované kabeláži Cat5e. Celá síť byla propojena centrálním switchem OvisLink Ether FSH2400R. Na tuto LAN už byly připojeny pracovní stanice zaměstnanců s operačním systémem Microsoft Windows 7, počítač s OS Windows v roli serveru a síťové tiskárny. Původně tuto LAN síť využívali pouze pracovníci školy. Na tomto serveru byly aplikace

k vnitřnímu fungování školy (účetnictví, pokladna, evidence, atd.). K internetu byla síť připojena přes adsl router a konektivitou od poskytovatele O2.

8.1.2 Modernizace

Škola požadovala vybudování bezdrátové sítě pro žáky tak, aby tito získali přístup na internet z mobilních telefonů, tabletů a notebooků. Toto zadání bylo dále rozvinuto a zároveň s touto sítí byla vytvořena bezdrátová síť pro zaměstnance. Z toho důvodu byly navrženy prvky podporující VLANy, které umožnily oddělit provoz stávající sítě LAN, Wi-Fi sítě pro zaměstnance a sítě pro studenty.

Ve škole došlo k vybudování bezdrátové sítě. Pro své vlastnosti a dobré možnosti správy byla zvolena zařízení UniFi AP, pracující na frekvenci 2,4 GHz. Pro pokrytí školy WiFi signálem bylo použito celkem 6 těchto zařízení. Pro připojení AP byla využita jak stávající strukturovaná kabeláž, tak kabeláž nově doplněná tak, aby bylo možno využít napájení přes centrální PoE panel, umístěného v datovém rozvaděči.

Z důvodu nedostatečné přípojné kapacity stávajícího switche byla síť doplněna o řiditelný, 24 portový Gbitový switch Zyxel GS1910-24.

Aktuálně jsou v provozu tři IP sítě, jejichž provoz řídí router Mikrotik RB450G. Zároveň je na tomto routeru v provozu firewall.

Došlo ke změně poskytovatele připojení a pro propojení s internetem je nyní řešeno přes WiFi.

8.1.3 Zabezpečení sítě

- Firewall

Na routeru Mikrotik RB450G, který zajišťuje přístup na internet, je v provozu firewall. Jsou na něm nastavena základní pravidla. Povoleny jsou porty 80(http), 443(https), 25(SMTP), 110(POP3), 143(IMAP). Port 53 (DNS) je povolen pouze z vnitřních sítí. Ostatní porty byly zakázány.

- Zabezpečení bezdrátových sítí

Při zabezpečování bezdrátové sítě bylo provedeno oddělení provozu do dvou oddělených bezdrátových sítí. První síť je určena pro zaměstnance školy a k připojení zařízení, které jsou součástí výuky. Druhá je navržena pro žáky a jejich zařízení jako notebooky a mobily a umožňuje jim prvořadě přístup k internetu. Zařízení Wi-Fi je

zabezpečena WPA2. Dále je zde užit zabezpečovací protokol TKIP. Autentizace klientů je provedena použitím předsdílených frází.

8.1.4 Zhodnocení zabezpečení:

Při hodnocení zabezpečení jsme museli brát na zřetel několik faktorů. V prvé řadě je nutné uvědomit si, že jde o síť malého rozsahu a pro popisovanou modernizaci byl vyčleněn jen malý rozpočet. Škola je navíc specificky zaměřená. Z toho důvodu nebyl přístup k internetu více omezen.

Zabezpečení počítačové sítě na této škole jsou na základní úrovni. Kladně lze zhodnotit oddělení provozu do tří sítí pomocí VLAN. Žáci tak mají přístup k internetu a zároveň nemohou běžným provozem ohrozit další zařízení k síti. Zaměstnanci školy tuto síť také využívají ovšem s možností komunikovat s ostatními zařízeními na síti. Na Wi-Fi je správně nastaveno nejnovější zabezpečení WPA2. Ovšem k zabezpečení správce sítě využil starší protokol TKIP, který je překonaný a představuje bezpečnostní riziko. Obě bezdrátové sítě používají různé přihlašovací klíče. Sporným bodem je autentizace klientů použitím předsdílených frází. Tady je opravdu na zvážení využití RADIUS serveru. S přihlédnutím k velikosti sítě, počtu osob, které se do sítě připojují a odlehlosti objektu, je tato volba dostačující.

Zabezpečení nastavená na routeru lze hodnotit jako základní. Na firewallu jsou povoleny pouze základní porty. Firewall však neobsahuje žádná pravidla pro filtrování provozu. Případný DDoS útok by mohl představovat vážný problém.

8.2 Výstavba druhé počítačové sítě

Druhá modernizace sítě, která je zde popisována, probíhala na větší škole s více jak 160 žáky a okolo 25 zaměstnanci. Modernizace probíhala od září 2014 až do června 2015. Použitá řešení jsou aktuální a mohla by sloužit jako modelový příklad, jak školu digitalizovat. Modernizace byla provedena na starší střední škole s odborným zaměřením. Na přání školy nebude z důvodu bezpečnosti daná škola jmenována.

Požadavek tohoto projektu bylo pokrytí školy Wi-Fi signálem a propojení počítačových učeben. Bezdrátová síť je určena pro zaměstnance i pro klienty (žáky). Modernizace proběhla v prosinci roku 2014 a byla zde použita moderní, ale zároveň osvědčená zařízení a prostředky:

Prostředky pro výstavbu sítě:

- Router CCR 1016.
- Switch CISCO 2950.
- Switch CISCO 2960.
- Wi-Fi Mikrotik RB 951.
- Wi-Fi UBNT Unifi.

Na škole bylo v rámci projektu Tablety pro vzdělávání rozšířena bezdrátová síť. Škola sídlí v budově, ve které již byla k dispozici kabeláž Cat6. O řízení sítě se stará router CCR 1016. Ve škole jsou dvě počítačové učebny. Zdejší počítače jsou do sítě připojeny přes dva Switche CISCO 2950. Na tyto Switche jsou připojeny i PC zaměstnanců. Ve škole byla zbudována bezdrátová síť. Zde byla použita Wi-Fi zařízení od společnosti Mikrotik a Ubiquiti.

8.2.1 Provedení sítě

Síť na této škole byla navržena jak pro zaměstnance, tak pro využívání studenty. Jelikož škola je tematicky zaměřena, síť je určena i pro firmu, která tuto modernizaci podporovala a která se stará o další fungování školy. Žákům byly školou zapůjčeny tablety pro připojení k internetu i školní LAN. Žáci mají také přístup k úložišti dat. Toto úložiště je zprostředkováno zařízením Synology DS1813+. Ve škole jsou dva servery pro zajištění fungování školy.

8.2.2 Zabezpečení sítě

Síť je střední až velké velikosti a do sítě má přístup velké množství lidí. Provoz na síti byl oddělen VLANkou do dvou LANek. První LAN je určena pro zaměstnance školy. V rámci této sítě mají přístup k zařízením určených výuce i internetu. Druhá síť je určena pro klienty školy (žáky).

- **Nastavení firewallu**

Stejně jako u předchozí sítě byl firewall zřízen na routeru Mikrotik zde typu CCR 1016. Na něm byly povoleny pouze doporučené porty a pravidla. Na něm jsou nastaveny port 80, port 443, port 22.

- **Zabezpečení bezdrátových sítí**

Při zabezpečování bezdrátové sítě bylo provedeno oddělení provozu do dvou oddělených bezdrátových sítí. Jedna síť je určena pro zaměstnance a umožňuje přístup zaměstnancům k zařízením. Zařízení Wi-Fi je zabezpečeno WPA2. Autentizace uživatelských zařízení probíhá přes předsdílenou frázi.

8.2.3 Zhodnocení zabezpečení

Pokud budeme hodnotit tuto síť z hlediska jejího zabezpečení, musíme v prvé řadě zmínit její velikost. Do sítě je připojeno velké množství zařízení.

Zabezpečení na této škole je na velmi nízké úrovni. Proti napadení zvenčí je síť chráněna pouze firewallem nastaveným na routeru, který má funkci řízení provozu v síti. To může představovat bezpečnostní problém i problém z hlediska rychlosti sítě. Vzhledem k velikosti, množství uživatelů a aplikacím, které na síti běží, je takovéto zabezpečení nedostatečné. Což se ukázalo při útoku na tuto síť.

Pozitivně lze hodnotit rozdělení provozu do dvou oddělených sítí. Za úvahu by stála možnost oddělit ještě síť pro zaměstnance pracující ve vedení, kteří mají přístup k citlivým informacím.

Další problém v tak velké síti představuje autentizace pomocí předsdílené fráze a volba zabezpečovacího protokolu TKIP. Tato volba znehodnocuje zabezpečení WPA2. K úložišti, které v této síti funguje, je zatím zajištěn přístup pouze webovým rozhraním. To používá šifrování HTTPS. Do budoucna se plánuje přístup přímo ze sítě, a proto je nutné

řešit ochranu, kterou na zařízení lze spustit. Jde především o Prevenci odmítnutí služby, Automatické blokování IP adres a Bránu firewall.

8.2.4 Návrhy na zlepšení

Na routeru, na kterém běží firewall, je nutné zavedení pravidel pro filtraci provozu. Na něm je třeba nastavit pravidla filtrování. Je nutné zabránit útokům, které jsem popisoval v teoretické části. Jak tuto filtraci provést, uvádí výrobce na svých stránkách. Pro tak velkou síť je vhodné pořízení specializovaného zařízení firewall.

Na Wi-Fi zařízeních je třeba změnit zabezpečovací protokol TKIP, je zastaralý, překonaný a jeho použití představuje bezpečnostní riziko. Dobrou náhradu představuje protokol AES. Vzhledem k vyššímu počtu lidí je nutné změnit způsob autentizace. Možný způsob přihlašování představuje autentizace RADIUS serverem.

8.2.5 Útoky na síť

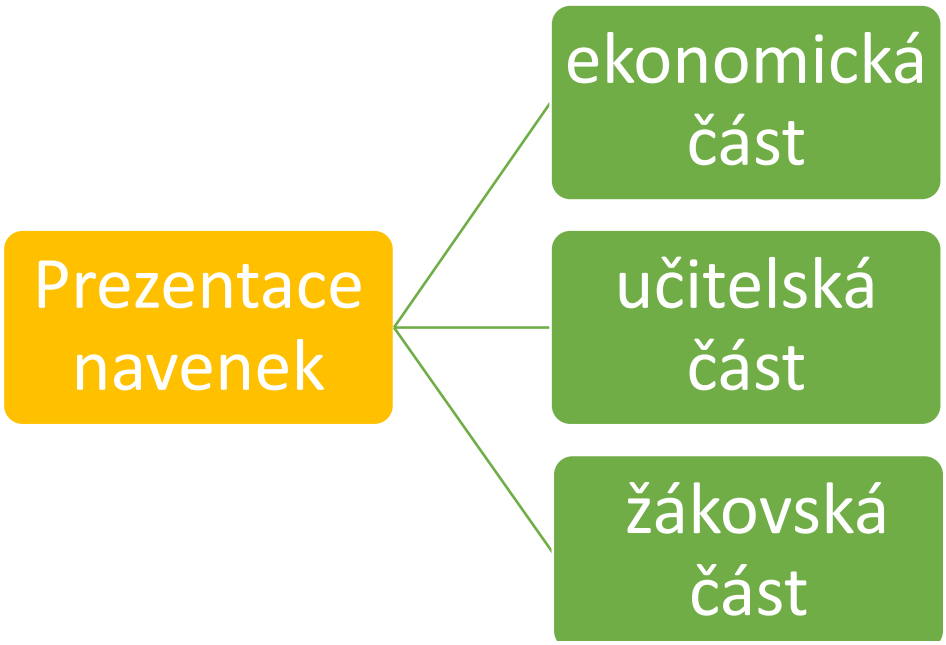
Na začátku roku 2015 došlo k útoku na tuto síť. Cílem tohoto útoku byl webový server, který měl na starost fungování některých aplikací a získaní dat. Útočník se snažil o přihlášení do systému přes protokol SSH. Pro přihlášení na server pomocí SSH bylo nutno zadat devítimístné heslo. Útočník použil útok hrubou silou a ve svém snažení byl úspěšný. Celý útok hrubou silou trval více jak 10 hodin. Po této době došlo k nalezení správného hesla. Na tomto serveru se zatím nenacházela žádná citlivá data, ale i tak došlo k nepříjemné situaci, neboť útočník tento stroj zneužil k spamování a DOS útokům na jiné stroje. Správci sítě se o tomto útoku dozvěděli, až když server začal spamovat další zařízení v internetu z nadměrného počtu navazovaných spojení. Tento problém nakonec byl vyřešen kompletní reinstalací napadeného systému a obnovou dat ze zálohy.

Útoku se dalo předejít nastavením filtrace provozu a logování ve firewallu. Takováto pravidla by umožnila zastavení přihlašování a zamezení provozu z útočníkovy adresy. V současnosti je k přihlášení nutné zadat více než 15místné heslo, to tvoří možných 256^{15} variací a je tedy prakticky nepřekonatelné. Zároveň firewallu bylo nastaveno logování a filtr který po x pokusech (řádově jednotky přihlášení) takový provoz zablokuje. I nadále je však síť nechráněná před útoky typu DDoS a dalších.

8.3 Vzorová školní počítačová síť

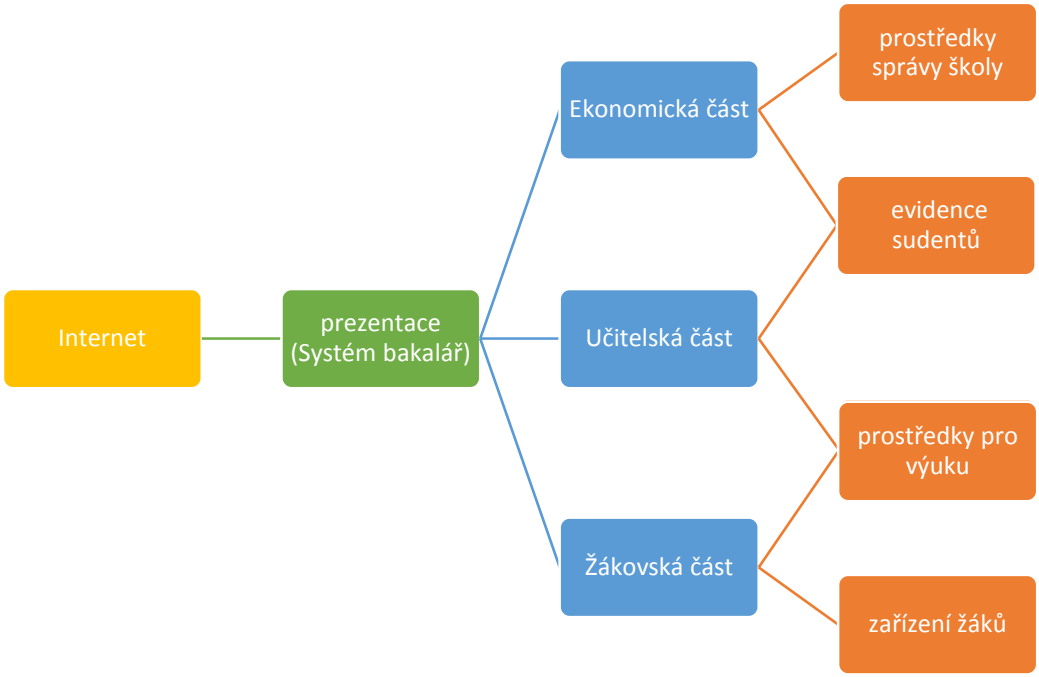
V této části jsme na základě teoretického studia a praktických poznatků navrhli vzorovou strukturu počítačové sítě. Daný model by měl být inspirací, jak vystavět školní počítačovou síť potřebné velikosti. Při tom odhlížíme od konkrétních typů zařízení. Jejich kapacity a výkony je třeba navrhnout podle požadavků konkrétní situace.

Každou školu je možné rozdělit na tři funkční části – ekonomickou, zajišťující administrativní provoz školy, učitelskou, které slouží k výuce a žákovskou. Pokud navrhneme strukturu výpočetní techniky a ostatních prostředků podle těchto částí, získáme strukturu pokrývající požadavky výše uvedených sekcí a zároveň hranice mezi nimi. Vytvořením takovéto struktury získáme základní vnitřní bezpečnost už na úrovni návrhu sítě.



Obrázek 10 Struktura školy (vlastní tvorba)

Pokud budeme reflektovat tuto strukturu, pak by počítačová síť mohla vypadat takto:



Obrázek 11 Struktura PC sítě školy (vlastní tvorba)

Pokud se nyní podíváme na provedení takové sítě, budeme z takové struktury vycházet. Je třeba vzít v úvahu možnosti sdílení prostředků. Při návrhu takovéto sítě bychom měli mít na paměti funkční nezávislost jednotlivých částí. Takový návrh nám zajistí funkčnost a jednoduchou správu celé LAN i při napadení nebo poškození jedné části. Proto bychom provoz v takové síti měli oddělit. Zároveň je vhodné mít v síti minimální možné množství zařízení.

8.3.1 Přístup k internetu

Tato část bude zajišťovat přístup jednotlivých částí. Při návrhu sítě je nutné zvážit a vybrat vhodný prostředek zajišťující rychlý a bezpečný přístup k internetu. Jelikož bude toto zařízení bránou k internetu, je velmi důležité toto zařízení zabezpečit. Toto zabezpečení by mělo obsahovat firewall, na kterém by měl být otevřeny pouze základní porty. Dále je běžné používání IPS sond pro ochranu serverů. Na zařízení by se pravidelně měly instalovat záplaty. V případě serverů je vhodné instalovat ověřený antivirus.

V další části se budu věnovat zabezpečení aktivních prvků v síti před útoky zevnitř.

Základní ochrana spočívá v ověření, kdo do naší sítě vstupuje. K tomuto ověření lze využít funkci Network Admission Control (NAC). Pro ověření použijeme standard 802.1x. Pro nejlepší zabezpečení budeme autentizovat uživatele pomocí EAP proti RADIUS serveru. Právě zde je vhodné oddělit provoz na síti pomocí VLAN.

Další obranou je využívání zabezpečeného přístupu na aktivní prvky a protokoly SSH nebo HTTPS.

Možným nebezpečím je podvržení DHCP serveru. Útočník na svém počítači spustí vlastní DHCP server a ostatním uživatelů začne přidělovat nesmyslné IP adresy. Zabezpečení tohoto zařízení je propojeno s vhodnou volbou zařízení switchů umožňující využít funkci DHCP snooping.

Nyní se už zaměřím na strukturu školy a od ní odvíjející se strukturu sítě.

8.3.2 Ekonomická část

Ekonomická část má funkci správy školy a evidence. Proto by i provoz na její části sítě měl tomu odpovídat. V této části dochází ke zpracování citlivých dat. Jak jsme naznačovali ve schématu, tento úsek má dvě hlavní náplně práce, správu školy a evidenci klientů, tedy žáků. Provoz by zde měl být od ostatních částí sítě oddělen a přístup povolit pouze osobám povolaným, jejíž okruh by měl být co nejmenší. Provoz na této části sítě by měl být šifrovaný. Pokud je v této části osazen server, měly by být na něm spuštěny pouze užívané aplikace. Část, starající se o evidenci žáků, je využívána jak ekonomickým oddělením, tak učiteli, to by mělo být zohledněno na databázové úrovni.

8.3.3 Učitelská část

Učitelská část má funkci výuky a evidence. Zaměstnanci, užívající tuto síť, využívají zařízení usnadňující výuku. Zároveň se k této části sítě připojují učitelé s vlastními zařízeními jako notebooky, mobily a tablety. To je velké množství zařízení a tedy i potenciálních problematických míst. Zároveň mají přístup k citlivým datům z evidence žáků, a proto nelze tuto síť odpojit od ostatních. Z těchto důvodů by i zde měl být provoz šifrován, přístup do evidence umožněn pouze z vybraných zabezpečených zařízení.

8.3.4 Žákovská část

Tato část slouží žákům k přístupu na internet a prostředkům, kteří žáci využívají ke studiu. Tato část je nejvíce problematická. Do této části se připojuje největší množství lidí s velkou množinou zařízení. Navíc musíme předpokládat, že do této sítě se budou připojovat lidé, kteří nebudou chápat a rozumět pravidlům bezpečnosti. Proto je vhodné mít tuto síť oddělenou od ostatních. Přístup do sítě autentizovat pomocí EAP proti serveru RADIUS. V našem schématu jsme zaznačili, že by žáci měli mít přístup k prostředkům pro výuku. Tento přístup by však měl být omezený a připojení k zařízením by mělo být povoleno prověřenou autentizací.

Závěr

Bakalářská práce přibližuje problematiku zabezpečení školních počítačových sítí.

Školní prostředí je specifické svým základním úkolem vzdělávat, podporovat tvořivost a rozvoj schopností žáků. Správci školních sítí musí počítat s různorodým prostředím a způsobem využití sítí. Je třeba vzít v potaz různou úroveň znalostí a schopností žáků. Požadavky na zabezpečení funkčního prostředí pro výuku a fungování školy jdou mnohdy proti zvídavosti a kreativitě studentů. Znemožnit snahy studentů o sebevzdělávání a samostatný rozvoj vědomostí by šlo přímo proti základní úloze školy vychovávat samostatné a tvůrčí osobnosti.

Teoretická část této práce čtenáře seznamuje s charakteristikou školní počítačové sítě. Jsou zde nadefinované důležité technologie počítačových sítí. Zároveň se školní síť porovnává se sítí podnikovou. Školní síť je otevřenější a přistupuje do ní v průměru větší množství lidí různými způsoby – stejný uživatel sítě může být připojen jednou přes ethernet, jindy přes Wi-Fi. Zajištění sítě se komplikuje i tím, že uživatel se může do sítě připojovat se zařízením patřícím škole nebo ze svého vlastního.

Pozornost byla věnována Wi-Fi sítím, jež se využívají u stále většího množství zařízení.

Hlavním úkolem této práce je ale především problematika zabezpečení. Práce popisuje technologii pro zabezpečení počítačových sítí. Předpoklad, že tato problematika se týká zejména přístupových bran, se potvrdil. Charakterizují se zde užívané technologie pro jejich zabezpečení i způsoby šifrování komunikace.

Práce se také zabývá aktuálními útoky hackerů. Ze studia problematiky vyplynulo, že většina útoků je založena na principech chyb ve fungování protokolů. Při vytváření této práce bylo zjištěno, že útoky na školní sítě jsou především cíleny na narušení jejího fungování.

V praktické části jsme porovnali počítačové sítě dvou odlišných škol co do stupně vzdělání, odbornosti, možnosti vybavení, velikosti. Ze zjištěných skutečností jsme došli k závěru, že zabezpečení školních počítačových sítí není příliš řešeno.

Nakonec jsme vytvořili strukturu modelové školní sítě. U toho jsme popsali možnosti jejího zabezpečení. Při návrhu struktury jsme brali v úvahu potřeby školy, jejich zaměstnanců i žáků a to tak, aby struktura sítě byla zároveň pilířem jejího zabezpečení.

Seznam bibliografických citací

1. BARKEN, Lee. *Wi-Fi: jak zabezpečit bezdrátovou síť*. Vyd. 1. Přeložil Jiří VESELSKÝ. Brno: Computer Press, 2004. ISBN 8025103463.
2. BOUŠEK, Petr. Počítačové sítě a jejich typy. In: *Www.Samuraj-cz.com* [online]. www.Samuraj-cz.com: www.Samuraj-cz.com, 2007 [cit. 2016-04-10]. Dostupné z: http://www.samuraj-cz.com/clanek/pocitacove-site-a-jejich-typy/
3. Co je VPN? *Microsoft technet* [online]. Microsoft: Microsoft, 2008 [cit. 2016-04-08]. Dostupné z: https://technet.microsoft.com/cs-cz/library/cc731954%28v=ws.10%29.aspx
4. *Co to je digitální certifikát* [online]. Interval.cz: Interval.cz, 2003 [cit. 2016-04-16]. Dostupné z: https://www.interval.cz/clanky/co-to-je-digitalni-certifikat/
5. ČÍŽEK, Jakub. *Meteorologové varují: Bezdrátový internet nám ruší radary* [online]. zive.cz, 2014-11-25, [cit. 2014-11-25].
6. *Elektronický podpis* [online]. sandbox.cz: Věra šumová, 2001 [cit. 2016-04-13]. Dostupné z: http://sandbox.cz/~varvara/El_podpis/index.html
7. FEIBEL, Werner. *Encyklopedie počítačových sítí* [CD-ROM]. Praha: Computer Press, 1996 [cit. 2016-04-09]. ISBN 80-85896-67-2.
8. Firewall. In: *Světhardware* [online]. světhardware: světhardware, 2005 [cit. 2016-04-08]. Dostupné z: http://www.svethardware.cz/slovnik/
9. HAVELKOVÁ, Ivana. *Bezpečnost počítačových sítí se zaměřením na Wi-Fi* [online]. Vysoká škola ekonomická v Praze, 2010 [cit. 2016-04-13]. Dostupné z: http://info.sks.cz/www/zavprace/soubory/68730.pdf
10. IDS/IPS. *4safety* [online]. 4safety: 4safety, 2011 [cit. 2016-04-08]. Dostupné z: http://www.4safety.cz/text/ids
11. JINDŘICH, Jelínek. *Úvod do počítačových sítí*. Ústí nad Labem, 2005.
12. KEJDUŠ, Radek. Test sedmi Wi-Fi routerů standardu 802.11ac: čtyřikrát rychlejší bezdrát. In: *Extrahardware.cz* [online]. Extrahardware.cz: Extrahardware.cz, 2014 [cit. 2016-04-18]. Dostupné z: http://www.cnews.cz/testy/test-sedmi-wi-fi-routeru-standardu-80211ac-ctyrikrat-rychlejsi-bezdrat
13. *Kroucená dvojlinka* [online]. Hardware počítačových sítí: Hardware počítačových sítí, 2012 [cit. 2016-04-13]. Dostupné z: http://hardwaresiti.webnode.cz/o-webu/

14. *Nastavení síťového routeru A-Z* [online]. pctunning: pctunning, 2008 [cit. 2016-04-18]. Dostupné z: http://pctuning.tyden.cz/software/jak-zkrotit-internet/11391-nastaveni_sitoveho_routeru_a-z_22?start=2
15. PEAK, Sean. Personal Firewall Software Reviews. In: *TopTenReviews* [online]. TopTenReviews: TopTenReviews, 2016 [cit. 2016-04-08]. Dostupné z: http://personal-firewall-software-review.toptenreviews.com/
16. PISKAČ, Pavel. Firewally. In: *Fi.muni.cz* [online]. Brno: Masarykova univerzita, 2008 [cit. 2016-04-08]. Dostupné z: http://www.fi.muni.cz/~kas/p090/referaty/2008-podzim/st/firewally.html
17. *Počítačová síť* [online]. ManagementMania.com: ManagementMania.com, 2011 [cit. 2016-04-15]. Dostupné z: https://managementmania.com/cs/pocitacova-sit
18. Popis symetrické a asymetrické šifrování. In: *Support.microsoft.com* [online]. Microsoft: Microsoft, 2007 [cit. 2016-04-08]. Dostupné z: https://support.microsoft.com/cs-cz/kb/246071
19. PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace: jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G. Vyd. 1. Brno: CP Books, 2005. ISBN 80-251-0791-4.
20. PUŽMANOVÁ, Rita. *TCP/IP v kostce*. 2., upr. a rozš. vyd. České Budějovice: Kopp, 2009. 619 s. ISBN 978-80-7232-388-3.
21. ROUBAL, Pavel. *Informatika a výpočetní technika pro střední školy: [kompletní látka pro nižší a vyšší úroveň státní maturity]*. Vyd. 1. Brno: Computer Press, 2010. 2 sv. (103, 112 s.). ISBN 978-80-251-3228-9.
22. ŘEHÁK, Jan. Co je to WiFi - úvod do technologie. In: *Vyvoj.hw* [online]. vyvoj.hw: Redakce HW serveru, 2003 [cit. 2016-04-15]. Dostupné z: http://vyvoj.hw.cz/produkty/ethernet/co-je-to-wifi-uvod-do-technologie.html
23. SATRAPA, Pavel. *Počítačové sítě* [online]. Liberec: 2008-06-27, [cit. 2008-09-05].
24. Seznamte se – DoS a DDoS útoky. *Security-Portal.cz* [online]. Security-Portal.cz: Security-Portal.cz [cit. 2016-04-09]. Dostupné z: http://www.security-portal.cz/clanky/seznamte-se-%E2%80%93-dos-ddos-%C3%BAtoky
25. Seznamte se – DoS a DDoS útoky. *Typy útoků používané hackery* [online]. michalspondr.webzdarma.cz: michalspondr.webzdarma.cz, 2012 [cit. 2016-04-

09]. Dostupné z: http://www.michalspondr.webzdarma.cz/hacking/typyutoku.html

26. *Síťové architektury* [online]. OWebu.cz: OWebu.cz, 2006 [cit. 2016-04-15]. Dostupné z: http://owebu.bloger.cz/Internet/Sitove-architektury
27. SOSINSKY, Barrie A. *Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]*. Vyd. 1. Brno: Computer Press, 2010. 840 s. ISBN 978-80-251-3363-7
28. SSID. *Tech-FAQ* [online]. Tech-FAQ: Tech-FAQ, 2012 [cit. 2016-04-09]. Dostupné z: http://www.tech-faq.com/ssid.shtml
29. ŠÍPEK, Petr. Zabezpečení WPS pro Wi-Fi není bezpečné. In: *Extrahardware.cz* [online]. Extrahardware.cz: Extrahardware.cz, 2012 [cit. 2016-04-18]. Dostupné z: http://www.cnews.cz/zabezpeceni-wps-pro-wi-fi-neni-bezpecne
30. ŠTRAUCH, Adam. Aircrack-ng: slovníkový útok na WPA-PSK. In: *Root.cz* [online]. Root.cz: Root.cz, 2008 [cit. 2016-04-18]. Dostupné z: http://www.root.cz/clanky/aircrack-ng-napadeni-wep-siti/
31. *The Firewall Toolkit* [online]. FWTK.ORG: FWTK.ORG, 2015 [cit. 2016-04-15]. Dostupné z: http://www.fwtk.org/
32. THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Vyd. 1. Brno: CP Books, 2005. 338 s. Cisco systems. ISBN 80-251-0417-6
33. *Útoky na přístup* [online]. Výučbový modul Cisco akademie: Výučbový modul Cisco akademie, 2010 [cit. 2016-04-13]. Dostupné z: http://www.tkelement.com/ktl/cvicenie_3_strana_3.php
34. WiFi sítě a jejich slabiny. *Security-Portal.cz* [online]. Security-Portal.cz: Security-Portal.cz, 2005 [cit. 2016-04-09]. Dostupné z: http://www.security-portal.cz/clanky/wifi-s%C3%ADt%C4%9B-jejich-slabiny
35. *Wikipedie: Otevřená encyklopedie: Firewall* [online]. c2015 [citováno 13. 04. 2016]. Dostupný z WWW: <https://cs.wikipedia.org/w/index.php?title=Firewall&oldid=13122622>
36. *Wikipedie: Otevřená encyklopedie: Počítačová síť* [online]. c2016 [citováno 10. 04. 2016]. Dostupný z WWW: <https://cs.wikipedia.org/w/index.php?title=Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5&oldid=13361932>

37. *Wikipedie: Otevřená encyklopedie: Symetrická šifra* [online]. c2016 [citováno 13. 04. 2016]. Dostupný z WWW: <https://cs.wikipedia.org/w/index.php?title=Symetrick%C3%A1_%C5%A1ifra&oldid=13225413>
38. *Wikipedie: Otevřená encyklopedie: Wired Equivalent Privacy* [online]. c2015 [citováno 5. 04. 2016]. Dostupný z WWW: <https://cs.wikipedia.org/w/index.php?title=Wired_Equivalent_Privacy&oldid=12780497>
39. *Wikipedie: Otevřená encyklopedie: Wired Equivalent Privacy* [online]. c2015 [citováno 9. 04. 2016]. Dostupný z WWW: <https://cs.wikipedia.org/w/index.php?title=Wired_Equivalent_Privacy&oldid=12780497>
40. WPA a WPA2. In: *Security-portal.cz* [online]. Security-portal.cz: Security-portal.cz, 2010 [cit. 2016-04-16]. Dostupné z: http://www.security-portal.cz/clanky/bezpe%C4%8Dnost-hacking-wifi-80211-4-%C4%8D%C3%A1st-wpa-wpa2
41. *Zabezpečení Wi-Fi sítí* [online]. 2008 [cit. 2010-03-26]. Soom. Dostupné z WWW: http://www.soom.cz/index.php?name=usertexts/show&aid=652

Seznam obrázků

Seznam použitých zkratek

AES	Advanced Encryption Standard, symetrická bloková šifra
AP	Access point (přístupový bod) základ Wi-Fi sítě
DES	Data Encryption Standard, symetrická šifra
DoS	Denial of Service, technika útoku na internetové služby či stránky
DDoS	distributed Denial of Service, je charakterizován zapojením většího počtu počítačů do útoku
EAP	Extesible Authentication Protokol
Ethernet	Souhrný název pro přenos dat po kabelovém vedení
IEEE	Institute of Electrical and Electronics Engineers
IEEE 802.11	IEEE 802.11 je standard pro Wi-Fi s dalšími doplňky pro lokální bezdrátové sítě
IDS	Intrussion Detection System, systém detekující narušení sítě
IPS	Intrussion Prevention systém, následník IDS
ISO/OSI	Referenční model organizace ISO, příklad řešení komunikace v počítačových a telekomunikačních sítích pomocí vrstevnatého modelu
LAN	Local Area Network - Lokální počítačová síť
MAN	Metropolitan Area Network – metropolitní síť
SMTP	Simple Mail Transfer Protocol, internetový protokol určený pro přenos zpráv elektronické pošty
SSID	Service Set Identifier - identifikátor bezdrátové sítě
SSH	Secure Shell, protokol pro zabezpečnou komunikaci
TCP/IP	Protokolová architektura definována sadou protokolů pro komunikaci v počítačové síti.
UDP	User Datagram Protocol, protokol ze sady protokolů internetu
VPN	Virtual Private Network
WAN	Wide Area Network, síť pokrývající rozsáhlá území
WEP	Wired Equivalent Privacy, zabezpečení bezdrátových sítí
Wi-Fi	Wirelless fidelity. Označení pro bezdrátové sítě
WLAN	Lokální bezdrátové sítě
WPA	Wi-Fi Protected Access
WPA2	WPA verze 2, nástupce WPA

ANOTACE

Jméno a příjmení:	Lukáš Kohout
Katedra:	Katedra technické a informační výchovy
Vedoucí práce:	Doc. PhDr. Miroslav Chráska, Ph.D.
Rok obhajoby:	2016

Název práce:	Problematika zabezpečení školní počítačové sítě
Název v angličtině:	The security issue of school computer networks
Anotace práce:	Tato bakalářská práce obsahuje informace o školních počítačových sítích, typech a charakteristice útoků na tyto sítě, technologiích a principech pro jejich zabezpečení, popis modernizace a užitých prostředků v reálném prostředí. V teoretické části práce jsou popsány základní charakteristiky školní počítačové sítě a bezdrátových sítí. V dalších částech jsou popsány prostředky a rady k zabezpečení sítě. Zabývám se také nejběžněji používanými útoky na bezpečnost sítě. V praktické části popisuji modernizaci a používané způsoby zabezpečení na počítačových sítích ve školách. Shrnuji zde, jak by měla vypadat školní síť z hlediska bezpečnosti.
Klíčová slova:	Školní počítačové sítě, síťové zabezpečení, útoky, síťové technologie
Anotace angličtině:	This thesis contains information about school computer networks, types and characteristics of attacks on these networks, overview of technologies and principles of security, description of modernization and tools used in a real environment. The theoretical part describes the basic characteristics of the school network and wireless networks. Next sections describe resources and advice for network security. I focused on the most commonly used attacks on network security. In the practical part I describe methods used for the modernization and security of computer networks in schools. Here I summarize, what should the school network fulfill in terms of safety.
Klíčová slova v angličtině:	School computer networks, Network security,attacks, networks technology
Přílohy vázané v práci:	-
Rozsah práce:	52 stran
Jazyk práce:	Český