Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Katedra systémové analýzy

Studijní program: Aplikovaná informatika

Obor: Informatika

Analýza zabezpečení bezdrátových sítí pro domácnosti

BAKALÁŘSKÁ PRÁCE

Student : Tomáš Švarc

Vedoucí : Ing. Ladislav Luc

Oponent : Ing. Pavel Strnad

2018

PROHLÁŠENÍ:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a že jsem uvedl všechny použité prameny a literaturu, ze které jsem čerpal.

V Praze dne 1. května 2018 . . . . . .

Tomáš Švarc

PODĚKOVÁNÍ:

Chtěl bych poděkovat svému vedoucímu Ing. Ladislavovi Lucovi, za cenné rady a poskytnutí profesionálního přístupu při vedení mé bakalářské práce. Následně bych rád poděkoval celému Oddělení síťové infrastruktury na Vysoké škole ekonomické vedené Tomášem Skřivanem, za pomoc, rady a motivaci při tvorbě této práce. Velké díky patří mé rodině za celoživotní obohacování, podporu a trpělivost.

Abstrakt

Tématem mé bakalářské práce je analýza zabezpečení bezdrátových sítí pro domácnosti. V mé práci jsem si stanovil několik cílů, kterých bych rád v práci dosáhl. Prvním cílem je v teoretické části co nejlépe seznámit čtenáře s danou problematikou, aby mohl využít poskytované informace pro osobní účely a bez problémů využívat bezdrátovou síť. Dalším cílem je uživatele informovat o kamerových systémech, alarmech a ovládání topení, které se dnes velmi často využívají bezdrátově. Třetím cílem je popsat možnosti a způsoby, jak docílit řádné ochrany dětí na webových stránkách a na počítači. Následně v práci vytvořím dotazník, který mi pomůže naplnit můj poslední vytyčený cíl a který má za úkol poukazovat, jaké zabezpečení uživatelé používají. Již zmíněným čtvrtým cílem je uvést modelový příklad zabezpečené sítě, který je vytvořen přehledně a jednoduše za účelem seznámení uživatele s tím, aby se nemusel obávat žádného napadení, zneužití, či odcizení osobních a citlivých dat.

Klíčová slova

Bezdrátová síť, Wi-Fi, zabezpečení bezdrátových sítí, IEEE 802.11, heslo

Abstract

The topic of my bachelor thesis is an analysis of security of wireless networks for households. I determined several goals that I would like to achieve. First goal is to inform readers with given issues in theoretical part. Provided information then might be used for personal purpose and for problem-free using of wireless network. Next goal is to inform about camera systems, alarms and heating controls that are very often these days. Third goal is to describe opportunities and ways how to attain children protection on computers and websites. Afterwards, I created a questionnaire that helped me fulfil my last goal and it pointed out what kind of security users use. The fourth goal is then to give a model example of secured network that is created clearly and easily in order to inform user that he doesn`t have to worry about any attack, misuse or stealing of personal data.

Keywords

Wireless network, Wi-Fi, security of wireless networks, IEEE 802.11, password

Obsah

1 Úvod

Téma mé bakalářské práce, která zní „Analýza zabezpečení bezdrátových sítí pro domácnosti“, jsem si vybral z několika důvodů. Jeden z nich je takový, že jsem vyrostl v rodině, která se správou a zabezpečením sítí již spoustu let živí. Další důvod mám proto, že pracuji v Oddělení síťové infrastruktury na Vysoké škole ekonomické v Praze, která se danou tématikou hodně zabývá, a proto si myslím, že tvorba této práce mě může v mnohém obohatit. Poslední motivace pro mě je seznámit se zmíněnou problematikou normální uživatele, kteří se ve světě informačních a komunikačních technologií trochu ztrácejí. Během svého života jsem se setkal s mnoho lidmi, kterým by se tyto informace mohly velmi hodit, a proto bych byl rád, kdyby moje práce mohla sloužit i jako takový návod.

Informační a komunikační technologie se neuvěřitelnou rychlostí vyvíjejí a v 21. století je to jedno z nejdůležitějších témat. Jakákoliv firma je v dnešní době na kybernetice závislá, jelikož se čím dál víc věcí přesouvá do elektronické podoby, a bez počítačů, notebooků, mobilů, tiskáren a dalších zařízení by byly společnosti bezradné. Písemná komunikace se začíná používat čím dál méně a téměř všichni mají v dnešní době email, Facebook, či využívají další počítačové programy. Všechny tyto programy je možné napadnout, a proto si musíme na kyberzločiny dávat velký pozor. I neznalí uživatelé počítačového světa znají pojem hacker. V době enormního rozmachu internetu se tito experti zaměřili převážně na vykrádání dat z osobních počítačů a serverů ve firmách a v domácnostech pomocí různých druhů virů. Bezdrátové sítě, které nás v dnešní době obklopují na každém kroku, dávají další šanci na odcizení tajných a citlivých informací. Ukradená data mohou být ve formě osobních či různých firemních informací (marketingové, technické, personální a mnohé další). A proto musíme dbát na bezpečnost a zabezpečení sítí. U bezdrátových sítí je zabezpečení obtížnější. V této práci se budu snažit nastínit, jak nejlépe těmto útokům zabránit.

2 Cíl práce

Cílem mé práce je doporučení, co vše by měl uživatel udělat, aby mohl provozovat domácí bezdrátovou síť s maximální ochranou proti napadení. Budu zde definovat pojmy, z kterých se bezdrátové sítě skládají, jaké jsou výhody a nevýhody Wi-Fi a jakými nástroji lze síť chránit. Následně se budu zabývat hlídacími kamerovými systémy, ovládáním topení, ovládáním alarmu a tématem ochrany dětí na webových stránkách a počítači. Jako modelový příklad uvedu co nejlépe zabezpečenou domácí síť složenou z nejnovějších technologií.

3 Bezdrátová síť

Bezdrátová síť, která je pro spoustu uživatelů známá pod názvem Wi-Fi (z anglického Wireless Fidelity), je typ počítačové sítě, která spojuje jednotlivé účastníky pomocí bezdrátové komunikace, převážně použitím elektromagnetických vln. V dnešní době je rozmach bezdrátových sítí obrovský a využívá se jak v domácnostech, ve firmách, ve veřejných prostorech tak i v telekomunikačních sítích. Pro uživatelskou Wi-Fi se používají dvě pásma, a to o frekvencích 2,4 GHz a 5 GHz. Institut inženýrů elektrotechniky („Institute of Electrical and Electronics Engineers – IEEE“) vyvíjí a schvaluje různé normy pro řadu počítačových technologií.

Obr. 1: Logo Wi-Fi

Zdroj: WI-FI ALLIANCE. Wi-Fi Logo.svg. In: Commons.wikimedia.org [online]. 2010 [cit. 2017-04-12]. Dostupné z: https://commons.wikimedia.org/wiki/File:Wi-Fi_Logo.svg

3.1 Historie bezdrátové sítě

Počátky bezdrátové komunikace můžeme nejvíce spojovat s Guglielmem Marconim. Tomuto italskému géniovi se podařilo roku 1895 informaci přenést bezdrátově na neuvěřitelnou vzdálenost přibližně dvou kilometrů. O šest let později v roce 1901 již došlo k prvnímu transatlantickému bezdrátovému přenosu dat. Následujícího vývoje v této oblasti jsme se dočkali díky námořnictvu, jelikož pozemní komunikace v té době kraloval telegraf. Přenášení informací bylo nejdříve pomocí Morseovy abecedy, avšak už v roce 1904 se uskutečnil první přenos hlasu. V desátých a dvacátých letech 20. století docházelo k velkému rozvoji rádiového vysílání. V USA se používaly mobilní rádiové stanice, které fungovaly v pásmu 2 MHz. Tyto stanice využívaly pouze vojenské a policejní složky. V roce 1924 bylo sestrojeno první mobilní rádio, které dokázalo přenášet hlas v obou směrech. Poté se v roce 1934 demonstrovala frekvenční modulace umožňující kvalitnější přenos zvuku. Velice důležitým vývojem si prošla bezdrátová komunikace během druhé světové války, kdy se využívala

přenosná rádio vysílačka společnosti Motorola. Po válce se objevily první návrhy moderních buňkových rádiových systémů a v roce 1961 byl proveden první analogový telefonní přenos. Již v 80. letech přišli první digitální telefonní systémy, z nichž nejúspěšnější byly v Evropě systémy GSM. V roce 1997 byl přijat standard IEEE 802.11, který má za úkol popisovat bezdrátovou komunikaci mezi počítači [1].

Obr. 2: Guglielmo Marconi

Zdroj: QRZ. Happy Birthday Guglielmo Marconi [online] 2016 [cit. 2018-03-28]. Dostupné z: http://qrznow.com/wp-content/uploads/2016/04/Immagini-Marconi1_fmt.jpeg

3.2 Zařízení pro provoz bezdrátové sítě

Jestli chceme vytvořit bezdrátovou síť, tak potřebujeme několik důležitých komponent. Jedním prvkem, pomocí kterého funguje Wi-Fi síť, je přístupový bod (Access Point), který vysílá a přijímá data. Toto zařízení má vlastní napájení a slouží i jako přepínač (ethernetový switch). V dnešní době mají minimálně jeden a více konektorů RJ45 pro propojení se stávající LAN sítí nebo pro vytvoření vlastní jednoduché LAN sítě. Některé technologicky vylepšené zařízení vlastní i konektory USB, díky kterým se mohou připojit do sítě tiskárny, přenosné disky a další zařízení. Poté potřebujeme pro dokonalou funkčnost bezdrátové sítě dobrou anténu. Existují tři typy antén a to směrová, všesměrová a sektorová. První zmíněná anténa je využívána k přenášení signálu do jednoho bodu na velkou vzdálenost, někdy se jedná i o několik kilometrů. Všesměrová anténa vysílá signál pod úhlem 360 stupňů na všechny strany. Tento typ se používá pro pokrytí menších prostorů a nalezneme ji nejčastěji. Sektorovou anténu najdeme hlavně tam, kde je potřeba pokrýt velký prostor. V souvislosti s anténami je důležitý parametr jejich ziskovost, který se uvádí v decibelech. Samozřejmě, že čím větší ziskovost u antény máme, tím je schopnější přijímat a vysílat signál na větší vzdálenost. Poté potřebuje pro provoz sítě tak zvanou Wi-Fi kartu (klientský adaptér), který využívá podobné principy jako síťová karta, pouze s tím rozdílem, že nepotřebujeme žádné kabely. Následně může záviset hodně na čipu ve

Wi-Fi kartě, který zpracovává již zmíněný signál z antény. Čím citlivější čip vlastníme, tím lépe si dokážeme poradit se signálem z větší vzdálenosti [2].

Tabulka 1: Antény

VZDÁLENOST	ZISK ANTÉNY
800-3000 m	7-9 dBi
3000-8000 m	9-15 dBi
8000-11000 m	15-20 dBi

3.3 Výhody a nevýhody Wi-Fi

Jednou z výhod bezdrátové sítě je to, že nemusíme k vybudování sítě využívat metalické kabely, tudíž máme o dost nižší náklady na vybudování sítě. V některých případech nelze ani kabelové propojení vytvořit (z důvodů stavebních či estetických). Jelikož přenos probíhá v bezlicenčním pásmu 2,4 GHz, tak nepotřebujeme ani žádný souhlas od příslušného úřadu. Dalším bonusem je to, že nemusíme být stále v jednom místě a můžeme se volně pohybovat v prostoru, kam Wi-Fi signál dosáhne. Jako největší nevýhodu bych uvedl, že již zmíněné bez licenční pásmo 2,4 GHz využívá i další zařízení jako například bluetooth, mikrovlnné trouby nebo bezdrátové telefony, tudíž může docházet k silnému rušení signálu. Čím více máme bezdrátových sítí v jedné lokalitě, tím se zvyšuje rušení používaného pásma. Dále může být signál ovlivněn problematickými klimatickými podmínkami mezi které patří třeba hustý déšť, sníh, bouřka a tak dále. Samozřejmě že přenosová rychlost u bezdrátových sítí je nižší než u pevných a také záleží na počtu připojených klientů. Další nevýhodou je zabezpečení bezdrátových sítí, které s běžnými komponentami jsou celkem snadno prolomitelné. V mé práci se proto budu zabývat touto tématikou, která je v dnešní době ve světě IT velmi diskutovaná [3].

3.4 Standardy IEEE 802.11

IEEE 802.11 je Wi-Fi standard s dalšími doplňky pro lokální bezdrátové sítě (Wireless LAN, WLAN). Norma IEEE 802.11 jako taková byla přijata v roce 1997. Tato norma fungovala na frekvenci 2,4 GHz a její maximální propustnost činila 2 Mbit/s. Následující změny normy byly označovány IEEE 802.11 High rate, která zvýšila rychlost na 11 Mbit/s. V roce 1999 se tato norma přejmenovala na IEEE 802.11b a také v tomto roce došlo k vytvoření normy IEEE 802.11a, která pracuje na frekvenci 5 GHz a samozřejmě logicky umožňuje vyšší rychlost. Standard IEEE 802.11g se schválila roku 2002 a z frekvenčního pásma 2,4 GHz je podporována stejnou rychlostí jako IEEE 802.11a a to 54 Mbit/s. Rok poté se začalo rozhodovat o standardu IEEE 802.11n, který se celých pět let schvaloval a byl roku 2008 schválen. Tento standard má přenosovou rychlost teoreticky až 600 Mbit/s, což se dokonce blíží k dnes používanému kabelovému standardu IEEE 802.3ab, který má 1000 Mbit/s. V roce 2013 se oznámil příchod standardu IEEE 802.11ac, který využívá obě pásma, jak 2,4, tak i 5 GHz. Nejnovějším standardem je 802.11ad. který přibírá pásmo 60 GHz [3].

Tabulka 2: Standardy IEEE

PŘEHLED STANDARDŮ IEEE 802.11				
STANDARD	**ROK VYDÁNÍ**	**PÁSMO [GHz]**	**MAXIMÁLNÍ RYCHLOST [Mbit/s]**	**FYZICKÁ VRSTVA**
původní IEEE 802.11	1997	2,4	2	DSSS a FHSS
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	600	MIMO OFDM
IEEE 802.11y	2008	3,7	54	
IEEE 802.11ac	2013	2,4 a 5	1000	MU-MIMO OFDM
IEEE 802.11ad	2012	2,4 , 5 a 60	7000	
IEEE 802.11ax	v budoucnu	2,4 a 5	10000	MIMO-OFDM

3.4.1 IEEE 802.11a

Tento standard, který je používán modulací OFDM, využívá Wi-Fi v pásmu 5 Ghz a poskytuje maximální teoretickou rychlost 54 Mbit/s. Ve srovnání se standardem IEEE 802.11b či IEEE 802.11g je stabilnější a vyspělejší. Má také povolený větší vyzařovací výkon, čímž lze používat na delší vzdálenost [3].

3.4.2 IEEE 802.11b

Tento standard je prvním zásadním dodatkem k normě IEEE 802.11 a jak jsem již uváděl, měl přídomek High rate, jelikož zvyšoval propustnost sítě na 11 Mbit/s. Byl schválen roku 1999 a navýšil rychlost oproti původnímu standardu na 11 Mbit/s v pásmu 2,4 GHz. V dnešní době je již tento standard zastaralý a nedostačující [1].

3.4.3 IEEE 802.11c

IEEE 802.11c je Wi-FI standard, který se věnuje přemosťování v bezdrátových sítích. Jedná se o doplňující standard IEEE 802.1D, který přidává požadavky na přemosťování Media Access Control (MAC), což je podvrstva linkové vrstvy. Standard IEEE 802.1D upravuje základní LAN standard pro 802.11 rámce [3].

3.4.4 IEEE 802.11d

Globální harmonizační standard, jak je tento Wi-Fi standard často nazýván, je používaný v zemích, kde nejsou povoleny systémy používající jiné dodatky standardu IEEE 802.11. Definuje požadavky na fyzickou vrstvu k uspokojení regulačních domén nepokrytých existujícími standardy. Liší se v povolených frekvencích, vyzařovacích výkonech a propustnosti signálu. Specifikace eliminuje nutnost vývoje a výroby určitých produktů pro různé země. Standard je proto vhodný pro ty systémy, které chtějí poskytovat globální roaming [3].

3.4.5 IEEE 802.11e

Tento standard je Wi-FI doplňkem ke standardu IEEE 802.11 vylepšující Media Access Control (MAC) podvrstvu linkové vrstvy rozšířením podpory kvalitu služeb (Quality of Service, QoS). Standard je důležitý pro aplikace, které jsou citlivé na zpoždění jako například Voice over Wireless IP a proudová multimédia [3].

3.4.6 IEEE 802.11g

Jedná se o Wi-Fi standard rozšiřující IEEE 802.11b, který je s ním kompatibilní a vysílá ve stejném frekvenčním pásmě (2400 – 2485 MHz) [3].

3.4.7 IEEE 802.11h

Je to Wi-Fi standard, který doplňuje standard IEEE 802.11a a je navržen s ohledem na evropské podmínky, aby bylo možné sítě využívat mimo budovy. Řeší problémy s rušením od ostatních zařízení, které pracují na 5 GHz frekvenci. Na tomto pásmu pracují třeba radary či satelitní systémy [3].

3.4.8 IEEE 802.11n

Tento Wi-Fi standard si klade za cíl upravit fyzickou vrstvu a část linkové vrstvy tak, aby se docílilo rychlosti přes 100 Mbit/s. Využívá se k tomu technologie MIMO, která je využívána vysílacími a přijímacími anténami [3].

3.4.9 IEEE 802.11r

Toto je doplněk standardu IEEE 802.11, který definuje rychlé přechody mezi BSS. Byl schválený roku 2008 a umožňuje připojení v pohybu, tudíž například ve vozidlech [3].

3.4.10 IEEE 802.11y

Stejné parametry jako u IEEE 802.11g jen s tím rozdílem, že pracuje na frekvenčním pásmu 3,7 GHz, což je pásmo v USA. U nás proto se s tímto standardem nesetkáme [2].

3.4.11 IEEE 802.11ac

Nástupce standardu IEEE 802.11n s teoretickou maximální rychlostí až 1000 Mbit/s. Na trhu se objevil od roku 2012-2015 [2].

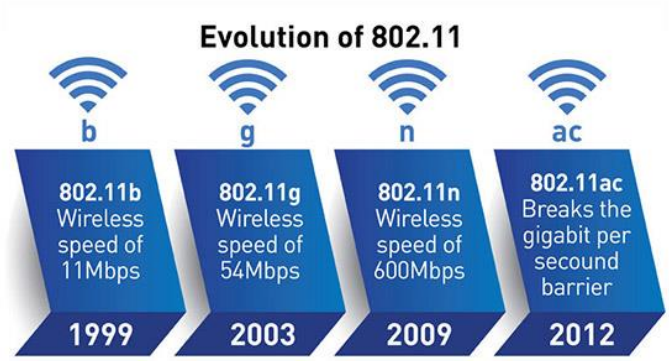
3.4.12 IEEE 802.11ad

Nejnovějším standardem je IEEE 802.11ad, který přibírá pásmo 60 GHz. Představen na trhu v roce 2016.

3.4.13 IEEE 802.11ax

Toto je pouze zatím návrh, který by měl mít maximální rychlost až 10000 Mbit/s. Představen by měl být podle známých informací někdy v roce 2019.

Obr. 3: Vývoj 802.11



Zdroj: STARHUB. Wireless Technologies & Limitations [online]. 2018 [cit. 2018-03-28]. Dostupné z: http://www.starhub.com/content/dam/starhub/2017/personal/support/broadband/broadband-101/wireless-technologies-limitations/evolution-of-802.jpg

4 Bezpečnost bezdrátové sítě

S bezdrátovými sítěmi se dnes setkáváme téměř na každém kroku, jak ve firmách, restauracích, tak hlavně v domácnostech. Pro normální rodinu je mnohem snazší vybudovat bezdrátovou síť a mít možnost se připojit odkudkoliv z rodinného domu či bytu než rozvádět po místnostech kabely. Samozřejmě ale nastává problém s tím, že umožňuje útočníkovi připojit se k internetu a přistupovat k našim datům. Zabezpečení Wi-Fi závisí nejvíce na tom, jaké jsou požadavky uživatelů. Znám bohužel i mnoho lidí, kteří se touto záležitostí vůbec nezabývají a tvrdí, že jejich bezdrátovou síť nemá důvod nikdo napadnout. Nebezpečí může nastat také z druhé strany, když se běžný uživatel připojí k nezabezpečené Wi-Fi například někde v restauraci, a začne surfovat po internetu. Je totiž dost možné, že síť je odposlouchávána neznámým útočníkem, který může naše data snadno odcizit. Poté hrozí nelegální činnost prostřednictvím naší bezdrátové sítě, jako je pořizování kopií filmů, her, programů a hudby. Za krádeže vznikají autorským společnostem milionové škody a orgány, které se zabývají vyšetřováním, nemají problém zjistit IP adresu přidělenou vaším ISP (Internet service provider) a na základě těchto údajů zjistit vaše jméno a adresu bydliště. Vyšetřovatelé se dostaví k vám domů a vinnu budou dávat pouze a jen vám, jelikož za aktivity na internetu je zodpovědný vlastník internetového připojení a má mít svoji síť zabezpečenou tak, aby tam neměl přístup nikdo cizí. Jak si můžete všimnout, hrozí spousty nebezpečí s touto tématikou, a proto se teď budeme zabývat tím, abychom těmto problémům předešli.

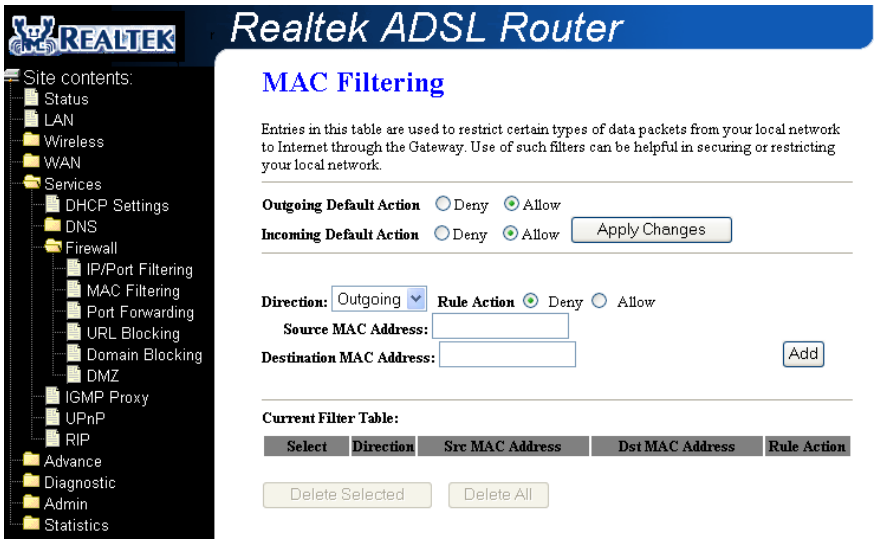
Obr. 4: Hackněte si svou bezdrátovou síť!

Zdroj: SVĚT ANDROIDA. Hackněte si svou bezdrátovou síť! [online]. 2014. [cit. 2018-03-28] Dostupné z: https://www.svetandroida.cz/media/2014/08/hacking_ico.jpg

4.1 Filtrování MAC adres

MAC adresa (Media Access Control) je jednoznačný identifikátor síťového zařízení, který používají různé protokoly druhé spojové vrstvy OSI. Tato adresa obsahuje hexadecimální tvar a také se ji říká fyzická adresa, jelikož je síťovému zařízení přidělena okamžitě při výrobě [1]. Nejčastěji ji známe jako šestici dvojciferných hexadecimálních čísel oddělených dvojtečkami. Zjištění MAC adresy v systému Windows je velmi jednoduché, a to pomocí příkazového řádku, který nalezneme většinou pod příkazem „cmd“. Po otevření dialogového okna napíšeme „ipconfig /all“, kde již nemáme problém fyzickou adresu najít. Každá MAC adresa je jedinečná a na celém světě nenajdeme žádné dvě zařízení, které by měly stejnou MAC adresu. Tuto adresu lze v dnešní době celkem snadno měnit, jelikož mnoho bezdrátových karet má ovladač, který tuto funkci umožňuje. Filtrování MAC adres je jedna z nejjednodušších forem zabezpečení bezdrátové sítě, přestože většina běžných uživatelů o tom nemá vůbec žádné tušení. Filtrování MAC adres se nastavuje v konfiguračním rozhraní přístupového bodu. Zjednodušeně to funguje tak, že v nastavení routeru se zadají adresy těch zařízení, které chceme, aby se připojovaly do naší bezdrátové sítě. Bohužel spolehlivost tohoto zabezpečení není příliš vysoká. Je to z toho důvodu, že povolená zařízení nejsou nijak skryta či šifrována. Jestli se tedy chce hacker dostat do sítě, stačí mu odchytit pár paketů při komunikaci povolených zařízení a pomocí šikovných programů zjistit povolenou MAC adresu. Poté už mu stačí jen změnit jeho adresu a přístup do sítě má umožněný. Proto se tento druh zabezpečení moc nevyužívá nebo se kombinuje s WEP, WPA či WPA2.

Obr. 5: Filtrování MAC adres



Zdroj: DOCPLAYER. WELL PTI-8511G. Uživatelská příručka [online]. 2016. [cit. 2018-03-28] Dostupné z: http://docplayer.cz/docs-images/24/3468679/images/31-0.png

4.2 Skrytí SSID

SSID neboli Service Set Identifier je identifikátor bezdrátové sítě Wi-Fi. Přístupový bod (access point) vysílá periodicky svůj identifikátor v takzvaném majákovém rámci (beacon frame) a klienti si tak mohou snadno vybrat, ke které bezdrátové síti se připojí. Parametr SSID se skládá z řetězců ASCII znaků, který obsahují maximálně 32 znaků. Tento parametr představuje klíč, kterým dochází ke spojení jednotlivých adaptérů v rámci bezdrátové sítě. Všechna bezdrátová zařízení pokoušející se o vzájemnou komunikaci mezi sebou musejí předávat tentýž SSID. Existují dvě hlavní varianty SSID, a to AD-HOC a infrastrukturní sítě. AD-HOC je bezdrátové připojení, které nemá přístupový bod (AP) a naopak infrastrukturní sítě tyto body obsahuje (popřípadě ESS – Extended Service Set). Skrytím SSID zabráníme tomu, aby bezdrátovou síť nemohl vyhledat někdo cizí, který do ní nemá přístup. Skrytí SSID je velmi jednoduchou formou zabezpečení stejně jako filtrování MAC adres. Toto zabezpečení ovšem není těžké prolomit. Kdykoliv se někdo chce přihlásit do této zabezpečené sítě, tak vysílá nešifrované SSID, aby se mohl připojit. Útočník už jen odchytí řetězec znaků a může se do sítě připojit. Proto se tento typ zabezpečení nepoužívá, a nebo jen v kombinaci s vyspělejším zabezpečením [4].

Obr. 6: Skrytí SSID

Zdroj: SVĚT IT. Jak zabezpečit domácí WiFi síť [online]. 2013. [cit. 2018-03-28]. Dostupné z: http://martasw.9e.cz/pictures/galleries/wifi01.jpg

4.3 Statické IP adresy

Další bezpečnostní opatření, který ztíží práci útočníkům, je vyžadování ručního nastavení IP adresy. Tato forma poskytuje velmi malou ochranu proti zkušeným útočníkům, ale méně zkušeným hackerům ztíží jejich průnik do sítě [5].

4.4 WEP

WEP (Wired Equivalent Privacy) je označení pro zabezpečení bezdrátových sítí podle původního standardu IEEE 802.11 z roku 1997. Cílem WEP bylo poskytnout zabezpečení obdobné drátovým počítačovým sítím, protože rádiový signál lze snadno odposlouchávat. V bezdrátové počítačové síti pracuje WEP na linkové vrstvě, kde šifruje přenášené rámce pomocí proudové šifry RC4. Díky tomu není lehké odposlechnout datový provoz přenášený v bezdrátový síti. Takzvaný 64bitový WEP používá 40 bitový klíč, ke kterému je připojen 24 bitový inicializační vektor a dohromady tak vytváří 64bitový RC4 klíč. Delší 128bitový WEP používá 104bitový klíč, ke kterému je připojen 24bitový inicializační vektor a dohromady tak tvoří 128bitový RC4 klíč. Někteří výrobci poskytují stejným způsobem i 256bitový WEP. Pro ověření integrity dat používá WEP kontrolní součty CRC-32. V dnešní době je však toto zabezpečení prolomeno (již roku 2001), i když nabízí mnohem lepší zabezpečení, než je třeba filtrování MAC adres či skrývání SSID. K rozluštění WEP je potřeba 5 až 10 milionů paketů, přičemž uživatel nesmí během toho WEP klíč měnit. Programy jako AirSnort a WEPCrack se zabývají komunikací mezi přístupovým bodem a klientem a slouží útočníkům k jejich nelegální činnosti. Další obrana může být využití dalšího šifrování a práce s autentizačními mechanismy jako například VPN či 802.1x. Mezi největší slabiny patří například to, že WEP klíč je na všech zařízeních v jedné WLAN. Dále také, že nepodporuje dynamickou změnu klíčů a že manuální změna WEP klíčů na všech zařízeních v případě velké firemní sítě není moc dobře realizovaná [6].

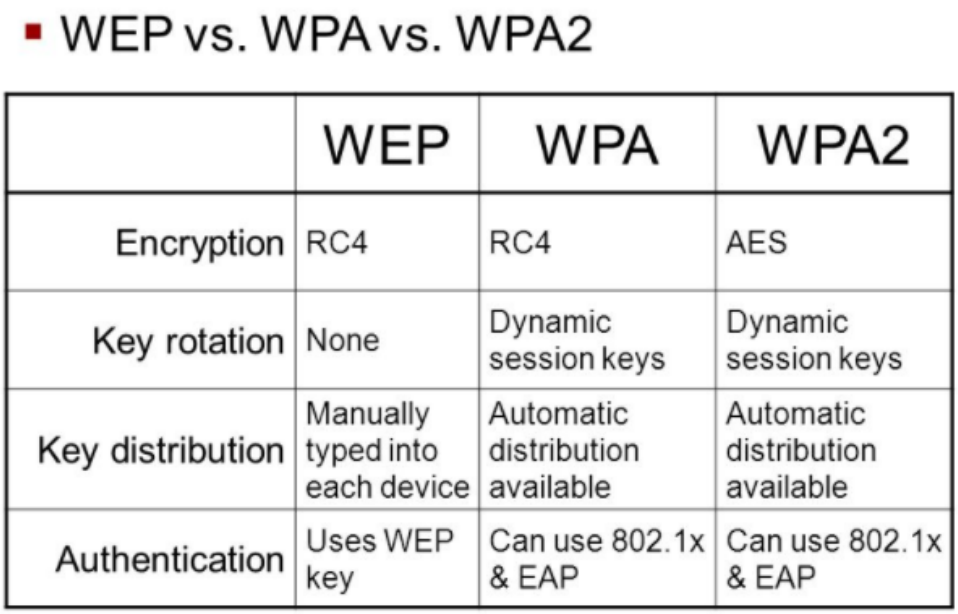
4.5 WPA

WPA (Wi-Fi Protected Access) se definovalo roku 2002 z důvodu prolomení zabezpečení WEP v roce 2001. WPA je vylepšený o šifrovací protokol TKIP (Temporal Key Integrity Protocol), který nabízí silné šifrování a řeší nedostatky, díky kterým se hackerům podařilo prolomit WEP. Další výhodou je dobrá správa šifrovacích klíčů, což umožňuje interní změnu šifrovacího klíče, aniž by někdo nový klíč odhalil. Také dochází ke změnám šifrovacích klíčů a útočník má mnohem méně času na zjištění a použití klíče. TKIP řeší nejvíce útoky, které jsou založené na kolizi, na podvržení, na útocích na slabé klíče a na opakovatelné útoky. WPA využívá 128 bitový šifrovací klíč a 48bitový inicializační vektor. Autentizace klienta je pro WPA navrženo buď použitím předsdílené fráze (Pre-shared key) nebo použitím autentizačního serveru (většinou Radius) pomocí protokolu IEEE 802.1x. Protokol 802.1x řeší slabiny jako chybějící správa klíčů, chybějící identifikace a autentizace uživatelů či chybějící centralizovaná autentizace a autorizace. V dnešní době je bohužel WPA také prolomeno, a proto je doporučeno používat bezpečnější protokol jako WPA2 [2].

4.6 WPA2

WPA2, známý také jako IEEE 802.11i, byl schválen 24.června 2004 a nahrazuje tak původní zabezpečení WEP, které bylo roku 2001 prolomeno a má mnoho bezpečnostních slabin. WPA2 využívá blokovou šifru AES (Advanced Encryption Standard) spolu s CCMP (Counter Mode with Block Chaining Message Authentication Code Protocol), který nahradil nedostačující šifrování RC4, který je spojován se zabezpečením WEP a WPA. WPA2 je v dnešní době nejlepším možným typem zabezpečení bezdrátové sítě. Bohužel v půlce října roku 2017 bezpečnostní experti z US-CERT a KU Leuven uveřejnili detaily týkající se prolomení šifrovacího protokolu WPA2. Objevili deset zranitelností a vytvořili i expolit KRACK (Key Reinstallation AtaCKs), který dokáže díry zneužít. Pomocí KRACKu by tak mohli odposlouchávat síťovou komunikaci, měnit obsah HTTP a podobně. Experti tvrdí, že zatím není nutné nahrazovat toto zabezpečení za jiné (které se asi v budoucnu bude jmenovat WPA3), jelikož pokud navštěvujete HTTPS weby, či využíváte VPN, prolomení WPA2 vám nehrozí. U webů běžících pouze přes http může hacker sledovat, co na internetu děláte a co všechno píšete.

Obr. 7: Srovnání WEP vs. WPA vs. WPA2



Zdroje: STAFFORD, Gilbert. Approaches to Mobile and Wireless Security [online]. 2016 [cit. 2018-02-26]. Dostupné z: http://slideplayer.com/slide/6216890/

4.7 WPS

V dnešní době mají téměř všechny domácí routery integrovanou funkci WPS (WiFi Protected Setup), což umožňuje jednoduché připojení bezdrátových zařízení do domácí sítě. WPS umožní nastavení sítě uživateli téměř bez jakýchkoliv znalostí, jelikož vůbec nemusí do webového rozhraní či nastavování DHCP. Tato funkce funguje tak, že stiskneme na routeru tlačítko s označením WPS či se symbolem šroubováku a router se přepne do odposlouchávacího režimu, při kterém zachycuje signály od vašeho notebooku či telefonu a umožní mu přístup do sítě bez jakékoliv autorizace. Jak můžete sami vidět, tato funkce není moc bezpečná, a proto výrobci vymysleli ochraňující mechanismus, který by měl WPS zabezpečit. Jedná se o osmimístné číslo, tak zvaný PIN, který se musí zadat pro ověření během odposlouchávání. Zmíněný PIN nalezneme většinou zespodu na Wi-Fi routeru.

Nejčastějším útokem na prolomení tohoto čísla je metoda Brute Force, což znamená v překladu útok brutální silou, který spočívá v tom, že se PIN uhádne. Útočník tedy posílá jednotlivé kombinace až do doby, dokud se do daného čísla netrefí. Normální osmimístné číslo poskytuje celkem 100 milionů kombinací, ale jelikož je tento PIN rozdělen na dvě poloviny, a ještě router odesílá informace o tom, která polovina je správná nebo ne, snižuje se počet kombinací na pouhých 11 tisíc. A to už zkušenému hackerovi netrvá příliš dlouho.

Zkušení odborníci proto doporučují, že nejjednodušší ochranou je tuto funkci vypnout. Ve webovém rozhraní routeru lze většinou WPS zakázat. Bohužel se ale u některých existujících modelů s vypnutím WPS nesetkáte, a tak router neustále poslouchá šum ve svém okolí a tím pádem je náchylnější k prolomení [16].

Obr. 8: WPS

Zdroje: STOBING, Chris. What is WPS [online]. 2018-01-01 [cit. 2018-04-09]. Dostupné z: http://www.gadgetreview.com/what-is-wps

4.8 Heslo

Heslo slouží k ověření totožnosti a autentizaci uživatele. Je to důležitý prvek, týkající se celkově bezpečnosti informačních technologií. Vytvoření silného heslo, které by nemělo být útočníkem nikdy prolomeno, musí splňovat několik základních kritérií, které si v této práci uvedeme.

Počet znaků musí obsahovat minimálně 8 znaků. Samozřejmě že platí, že čím více znaků heslo obsahuje, tím náročnější je nabourání útočníkem. Důležitá je kombinace malých a velkých písmen, číslic a speciálních znaků. Dále se musíme vyvarovat snadno zjistitelným heslům, mezi které patří jména příbuzných, partnerů, rodná čísla či data narození. Není doporučeno ani používat jednoduše dohledatelné slovo ve slovnících. Ukládání hesel je také jedno z možných rizik, které danému uživateli hrozí. Půjčování hesel či nalepení hesla v blízkosti počítače ztrácí celkovou pointu tohoto zabezpečení. V praktické části vám tuto tématiku ještě více nastíním a uvedu programy, které slouží pro bezpečné a jednoduché ukládání hesel. Pravidelné měnění hesel a využívání stále nových kombinací vylepšuje bezpečnost hesla.

Příklad vytvoření silného hesla může být z vašeho oblíbeného filmu, říkanky, vzpomínky či informace, kterou si vy osobně lehce zapamatujete. Když vezmeme v potaz například film Na samotě u lesa, písmeno O zaměníme za nulu, písmeno E za číslo tři, písmeno L za vykřičník a písmeno A za číslo čtyři. Upravený tvar hesla poté vypadá N4s4m0t3u!3s4, což se na první pohled uživateli může zdát velice složité, ale pomocí těchto mnemotechnických pomůcek si ho uživatel může lehce zapamatovat.

Mezi špatné heslo, které byste neměl nikdy používat, je například heslo12345, Monika123, či opsaní nebo zkopírování uživatelského jména jako hesla. Každý, kdo bude mít zájem heslo prolomit, tyto varianty začne používat, a i nepříliš zkušený útočník má šanci prolomit vaše přihlášení.

Dále bychom se měli přihlašovat pouze na stránkách HTTPS, které jsou bezpečně zašifrovány a zabezpečeny. Útočníci totiž na stránkách, které mají pouze HTTP, mohou jednoduše odposlouchávat komunikaci a nemají tudíž velký problém vaše citlivé informace zjistit [17].

Existuje několik způsobů, jak útočník zjistí vaše heslo. Některé z nich využívají silný výpočetní výkon zařízení, ale některé pouze důvěřivost a naivitu uživatelů.

Prvním způsobem je dnes často skloňovaný phishing, kdy se vás útočník snaží nalákat přes nastrčenou důvěryhodně vypadající webovou stránku, na kterou vás odkáže třeba email či sociální sítě. Pokud se necháte napálit, heslo útočníkovi poskytnete sami. Proto si můžeme všimnout, že například banky často upozorňují na hrozící riziko a to, že se hesla mají vyplňovat pouze a jen na oficiálních stránkách bank. Útočníci jsou totiž schopni vytvořit stránky, které vypadají úplně totožně, ale jejich webová adresa se neshoduje.

Druhým způsobem je pomocí slovníkového útoku. Existují databáze, které obsahují nejpoužívanější hesla a které útočník bude zkoušet jako první. Když vezmeme v potaz česká slova, nalezneme ve slovníku pouze více než 250 000 slov, které není problém porovnat i s průměrně výkonným počítačem během krátké doby.

Poslední variantu známe jako hrubou sílu (brute force). Jednoduše řečeno se vyzkouší všechny možné varianty. Tato možnost vyžaduje obrovský výpočetní výkon a může jít o časově velmi náročný proces. Prolomení touto variantou záleží samozřejmě na síle hesla, o které jsme se již v této kapitole bavili. Pro představu zde uvedu tabulku, která uvádí, jaké časové horizonty trvá jednotlivě silná hesla probourat pomocí využití průměrného počítače [18].

Tabulka 3: Síla hesel

HESLO TVOŘÍ:	POČET ZNAKŮ	DÉLKA HESLA								
		2	3	4	5	6	7	8	9	10
ČÍSLA	10	hned	hned	hned	hned	hned	1s	10s	1m40s	17m
JEN MALÁ/JEN VELKÁ PÍSMENA	26	hned	hned	hned	1s	31s	13m	6h	6d	163d
JEN MALÁ/JEN VELKÁ PÍSMENA + ČÍSLA	36	hned	hned	hned	6s	4m	2h	3d	118d	12r
MALÁ + VELKÁ PÍSMENA	52	hned	hned	1s	38s	33m	1d5h	62d	9r	458r
MALÁ + VELKÁ PÍSMENA + ČÍSLA	62	hned	hned	2s	2m	1h35m	4d	253d	43r	2661r
MALÁ + VELKÁ PÍSMENA + SPEC. ZNAKY	85	hned	hned	5s	7m24s	10h	37d	9r	734r	6248r
MALÁ + VELKÁ PÍSMENA + ČÍSLA + SPEC. ZNAKY	95	hned	hned	8s	13m	20h	81d	21r	1999r	189858r

5 Doporučení pro zabezpečení přístupu

V této části bych rád shrnul, co vše má uživatel udělat, aby byla jeho bezdrátová síť co nejbezpečnější a nejlépe zabezpečená. Bohužel se i v mé generaci najdou tací, kteří mi dokážou tvrdit, že oni nemají v síti nic důležitého, a že jim nemůžou nic ukrást. Zcizení dat ale není jenom jediné riziko, které může hrozit. Útočník může odposlouchávat vaši komunikaci, přistupovat ke sdíleným souborům, může kontrolovat a ovládat další zařízení v síti, může přistupovat na internet a může pod vaší identitou spáchat nějaký trestný čin. Jak již jsem zmiňoval v mé práci, odpovědnost za jeho napáchané škody nebude na nikoho jiného než na vás. Proto si myslím, že touto tématikou by se měl zajímat každý uživatel, a to bez výjimky [8].

Nejdůležitější a základní způsob zabezpečení bezdrátových sítí je pomocí šifrování přístupu. Bez znalosti šifrovacího klíče má útočník velké problémy prolomit přístup. Výše jsme si uváděli, že nejsilnější a nejnovější šifrovací protokol je WPA2, který je s kombinací silného hesla téměř neprolomitelný.

Poté je velmi důležité nastavení již zmíněného silného hesla. Mělo by být dostatečně dlouhé, těžko odhadnutelné a mělo by obsahovat jak velká a malá písmena, tak i číslice a nepísemné znaky. Běžné uživatelské heslo by mělo obsahovat alespoň osm znaků, které už je v kombinaci s protokolem WPA2 velmi bezpečné. Existují mnohá doporučení, jak si nastavit silné heslo, tak aby bylo i dobře zapamatovatelné.

Následně je doporučeno si změnit přihlašovací jméno a heslo pro přístup do konfigurace bezdrátového zařízení (routeru, access pointu). Obvykle se totiž setkáváme s továrním nastavením admin / admin, což je velmi snadno prolomitelné. Doplňkově lze také změnit IP adresu routeru, jelikož výrobci většinou nastavují výchozí 192.168.1.1.

Dále existují ochrany zabezpečení, které jsme již uváděli, a to filtrování MAC adres či zakázaní vysílání názvu sítě (SSID). Rád bych také zmínil technologii WPS (wi-fi protected setup), která umožňuje bezpečné připojování a nastavování domácí bezdrátové sítě. Hlavním cílem je ochrana uživatelských dat a velmi jednoduchá konfigurace Wi-Fi sítě. Pro ochranu se využívá osmimístný PIN, kterým se identifikují uživatelé.

6 Kamerové systémy a alarmy

Dalším tématem, kterým bych se chtěl zabývat a velmi souvisí s bezpečností, jsou kamerové systémy a alarmy. Pokud nejste miliardář, který vlastní svoji vlastní ochranku, či nemáte zdatného hlídacího psa, určitě se vám bude hodit některý z kamerových a alarmových bezpečnostních systémů, abyste mohli ochránit své nejbližší a svůj majetek. Alarmy jsou již dnes bezdrátově propojené s čidly, která mohou být umístěny v různých částech domu bez nutnosti kabelových rozvodů. Alarmy jsou pro případ poplachu vybaveny sirénou, ale také mají možnost pomocí GSM komunikátoru zavolat váš mobilní telefon či zaslat SMS zprávu o poplachu nebo jiné události. Při napojení na pult centralizované ochrany je během několika minut přivolána bezpečnostní služba. Díky těmto systémům velmi zbohatl Dalibor Dědek, který je majitelem firmy Jablotron, která pochází z mého rodného města Jablonce nad Nisou. Ovládání těchto zařízení je velmi jednoduché, přehledné a praktické. Nastavení požadovaných funkcí je samozřejmě na každém uživateli, jak si to bude přát. Alarmy umožňují střežit jednotlivé části domu, umí ovládat různé spotřebiče či případně vyslat tísňový signál [9].

V dnešní době se těší stále větší oblibě tak zvané IP kamery, které mohou být i bezdrátové. Pomocí IP kamer můžeme sledovat jejich snímaný obraz z jakéhokoli místa prostřednictvím webového rozhraní. Bezdrátové IP kamery mají výhodu nejen v tom, že nemusíme vést ke každé kameře zbytečné kabely, ale i to, že není problém, když chceme kamerový systém rozšířit. Samozřejmě se ale opět vracíme k zabezpečení, jelikož komunikace probíhá přes internet, který může být útočníkem napaden. Kromě bezpečnostních opatření bezdrátové sítě, které jsem již uváděl, máme nadstandartní zabezpečení, a to ve formě změněného hesla při nastavení všech kamer, což mnoho uživatelů nedělá a nechává standartní výchozí heslo, které není obtížné prolomit. Dále doporučuji aktualizovat firmware od výrobce IP kamer, který by měl zaručovat lepší a novější funkce, a tudíž i vyšší bezpečnost. Nakonec bychom se měli zabývat i port forwardingem, který může sloužit jako jedna z dalších základních ochran proti hacknutí vaší IP kamery. Pro zjednodušení k nezasvěceným uživatelům stačí říct, aby vždy použili jiné porty, než jsou továrně nastaveny ve vaší IP kameře [10].

7 Ovládání topení

Tak zvané Wi-Fi termostaty představují novinku v oblasti regulace obytných budov. Nabízí stejné standardy jako běžné termostaty, akorát na rozdíl od nich je lze ovládat například pomocí chytrého telefonu odkudkoliv prostřednictvím bezdrátové sítě. Aplikaci, která umožňuje komunikaci s těmito zařízeními, lze stáhnout jak pro Android, iOS, tak i pro Windows Phone. Systémy mají obvykle dokonce i exkluzivní funkci, která dokáže automaticky rozeznávat pohyb jednotlivých členů domácnosti (podle jejich chytrých telefonů), a když poslední člen opustí byt, systém automaticky sníží teplotu. Opačně, když se první člen domácnosti blíží k domovu (je možno nastavit i vzdálenost) systém automaticky teplotu zvýší opět na komfortní úroveň [11].

Obr. 9: Wi-Fi termostaty

Zdroj: UNISHOP. WiFi termostat [online]. 2018. [cit. 2018-03-28]. Dostupné z: http://www.uni-shop.cz/fotky1449/fotos/_vyr_782NEO_kit_00.jpg

8 Ochrana dětí na webu

Děti začínají využívat internet mnohem dříve, než by bylo ve spoustě případů vyhovující. V této pasáži si povíme, jak chránit své děti před různými nástrahami internetu, jak blokovat přístup na nebezpečné webové stránky, jak měřit strávený čas u počítače, či jak sledovat dění na webových stránkách.

Na internetu může vládnou anarchie, pornografické stránky a různé seznamky s návštěvníky, kteří mohou mít pedofilní sklony. Když to porovnáme s televizním nebo rozhlasovým vysílán, kde se neobjeví žádný nevhodný materiál před desátou hodinou večerní, internet je na tom mnohem hůře. Obsah je po několika kliknutí přístupný téměř komukoliv a kdykoliv. Další hrozbou je to, že kdokoliv si může vytvořit libovolnou identitu, pomocí které může zneužívat například lidské city.

Dnes již známe spoustu chytrých programů, kteří nám s touto tématikou dokáží pomoci. Filseclab Internet Guardian Angel je software, který filtruje prohlížení obsahu pomocí kontroly TCP/IP protokolu. Umí filtrovat erotické stránky, chat, online hry, blokovat pop-up okna a mnohé další. Dalšími známými nástroji jsou Any Weblock, Naomi, Web Blocker a tak dále. Všechny fungují na podobném principu, kde máte možnost filtrovat obsah stránek. Nástroje iProtectYou a Anti-Porn dokáží ještě omezovat strávený čas u počítače a nemají problém zařízení po určité době vypnout. Šikovná aplikace i-bezpecne.cz má vytipováno celkem přes 1 300 000 nevhodných stránek, které se rozdělují do různých kategorií a rodiče poté mohou blokovat ty, které uzná za vhodné.

Jestliže ale chceme chránit své děti, nemusíme ani žádný nový software stahovat. Operační systém Windows nám totiž umožňuje tak zvanou rodičovskou kontrolu, který umožňuje blokovat například webovou adresu. I prohlížeč Internet Explorer má nástroje, pomocí kterých lze zakázat nebezpečné adresy. Další možnost je pomocí routeru, kde v konfiguraci můžeme vesele zakazovat.

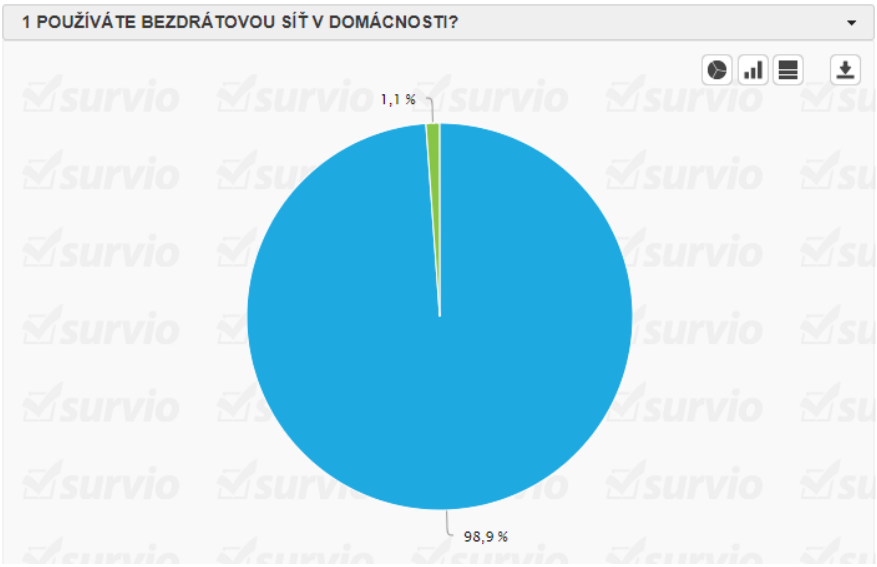
Dále bych rád zmínil program Synthetic End User Monitor, který dokáže nahrávat a sledovat pohyb uživatele po webu. Velmi šikovný je program BlackBox, který zapisuje každou spuštěnou aplikaci, každý záznam o navštívené stránce, každý záznam o vyhledávání textu na webu, dobu využití času na počítači, záznamy obrazovky či záznamy komunikačních zpráv [12] [13].

9 Průzkum bezdrátových sítí

Svůj průzkum vztahující se k tématu bezdrátových sítí jsem vytvářel proto, abych se přesvědčil o tom, jaké zařízení uživatelé používají v domácnostech, jaký typ zabezpečení vlastní, jak silné heslo mají a tak dále. Dotazník jsem vygeneroval online na internetu pomocí tak zvaného Survia, který je zdarma, a je ideálním nástrojem pro rychlé a jednoduše vyhodnocované dotazníky. Pro rozeslání dotazníku z důvodu sběru dat jsem využíval převážně sociální sítě Facebook, Instagram a také elektronickou poštu, ve které byl na můj dotazník odkaz. Celkově jsem nasbíral téměř sto respondentů, což je k mému účelu vyhovující a mohu tedy správně analyzovat výsledky. Dotazník byl dispozici k vyplnění od února roku 2018, tudíž respondenti měli celé dva měsíce na to dotazník vyplnit. V rámci průzkumu bylo uvedeno celkově sedm otázek pro všechny typy uživatelů. Nakonec bych rád své výsledky porovnal s těmi, které byly vytvořeny před několika lety a tím mohl určit, jak se vyvinulo zabezpečení bezdrátových sítí v domácnostech.

První otázka, kterou jsem uživatelům položil, se zabývá tím, zdali používají v domácnosti bezdrátovou síť. Je vidět, že v dnešní době si život bez internetu nedokážeme představit, což dokazuje výsledek, kdy celkově 98,9% lidí uvedlo, že doma bezdrátovou síť využívá.

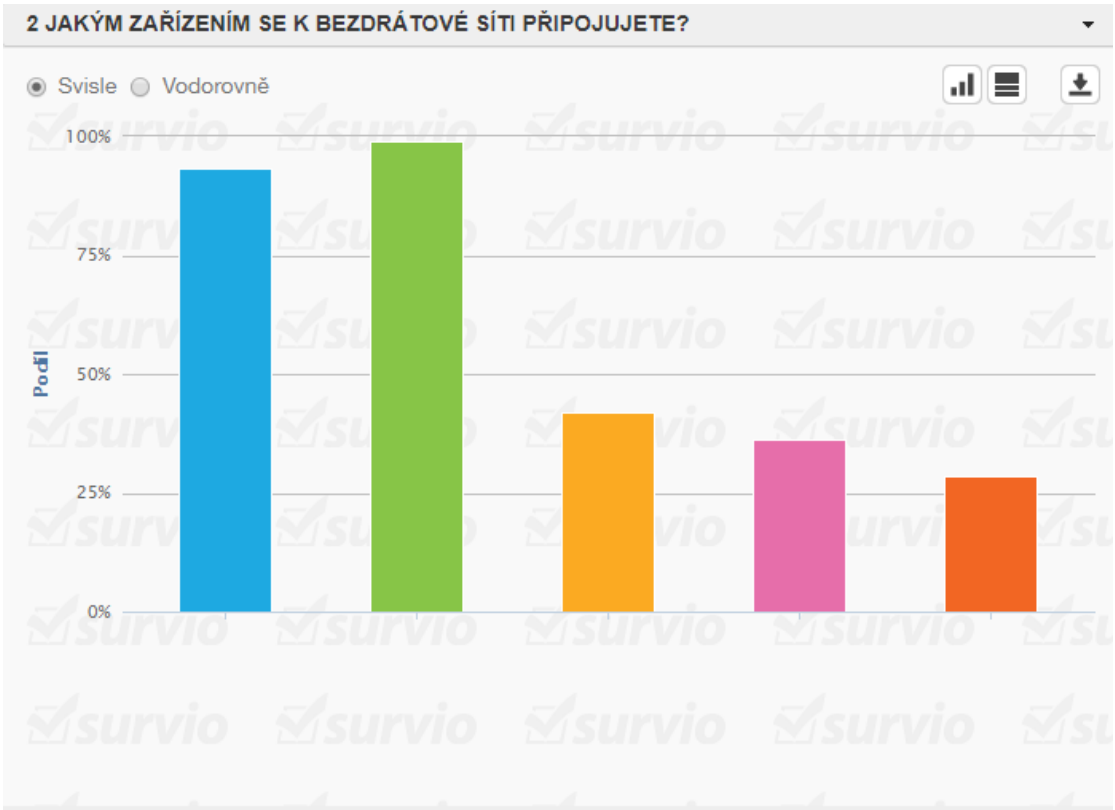
Obr. 10: Použití bezdrátové sítě v domácnosti



Zdroje: AUTOR. Prostřednictvím portálu SURVIO. 2018. Dostupné z: https://www.survio.com/survey/d/S5G7R7C5B7H9L8C9V

Následně mě zajímalo, jakými zařízeními se v domácnostech lidé připojují, protože mobilní telefony, počítače, televize i tablety nemají úplně stejný druh zabezpečení. Bezpečnost při práci musíme přizpůsobit konkrétnímu zařízení. Mobilem se připojují všichni respondenti, kteří mají bezdrátovou síť v domácnosti. Notebook a PC má také velké zastoupení, a to přes 94%. V posledním desetiletí se velmi rozšířily tablety, které používá v domácím prostředí 42% uživatelů. Chytré televize také nezaostávají a podíl využívání se vyhoupl přes 36 %. Poté se ještě lidé připojují do bezdrátové sítě pomocí tiskáren či hodinek, což zaškrtlo celkem 28,4% respondentů.

Obr. 11: Využívané zařízení v bezdrátové síti

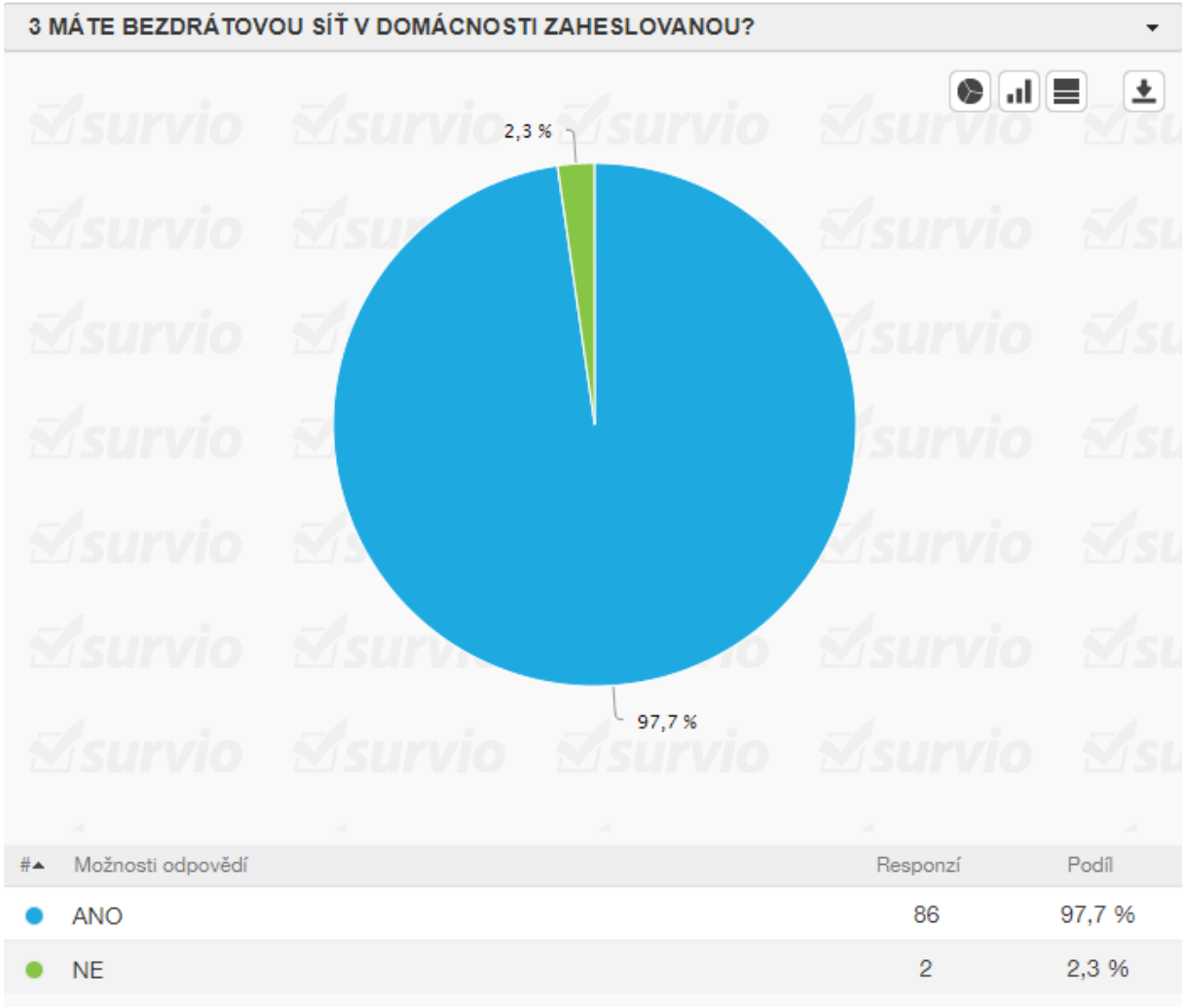


#	Možnosti odpovědí	Responzí	Podíl
●	NOTEBOOK, PC	82	93,2 %
●	MOBILNÍ TELEFON	87	98,9 %
●	TABLET	37	42,0 %
●	TELEVIZE	32	36,4 %
●	OSTATNÍ ZAŘÍZENÍ (hodinky, tiskárny,...)	25	28,4 %

Zdroje: AUTOR. Prostřednictvím portálu SURVIO. 2018. Dostupné z: https://www.survio.com/survey/d/S5G7R7C5B7H9L8C9V

Třetí otázka se zabývá již zabezpečením přístupu do sítě, a to přesněji heslem. Celkově 97,7% uživatelů uvedlo, že ve své bezdrátové sítě má heslo, což mi přijde velmi uspokojující výsledek.

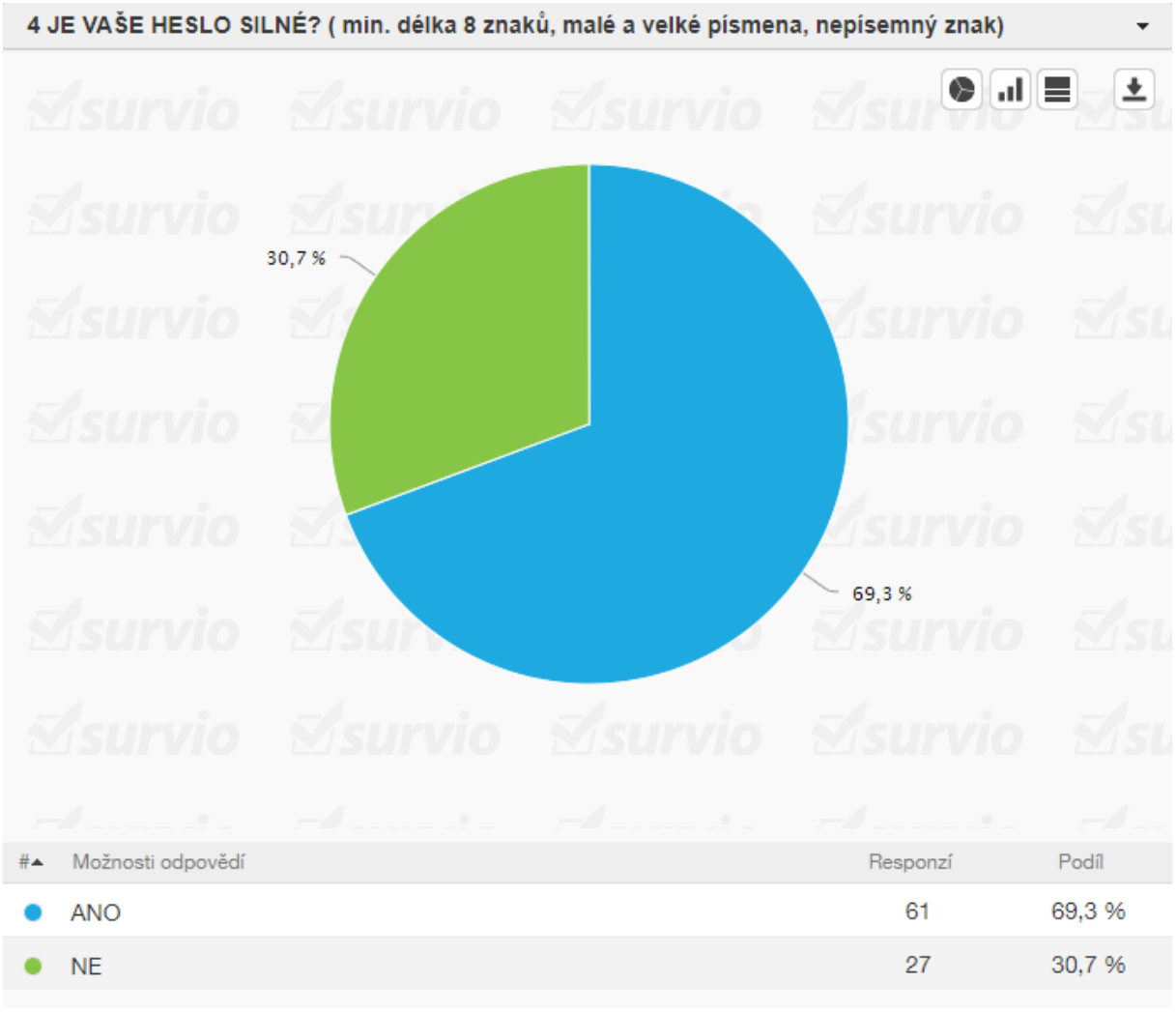
Obr. 12: Zaheslovaná bezdrátová síť v domácnosti



Zdroje: AUTOR. Prostřednictvím portálu SURVIO. 2018. Dostupné z: https://www.survio.com/survey/d/S5G7R7C5B7H9L8C9V

Poté jsem se zajímal o to, jak silné heslo do sítě uživatelé mají. Aby měl útočník problém heslo prolomit, mělo by obsahovat minimálně osm znaků, přičemž by jeho součástí mělo být aspoň jedno velké, jedno malé písmeno a jeden nepísemný znak. Výsledek mě mile překvapil, jelikož celkově téměř 70% tento požadavek splňuje. Čím delší heslo, tím samozřejmě bude hackerům prolomení déle trvat.

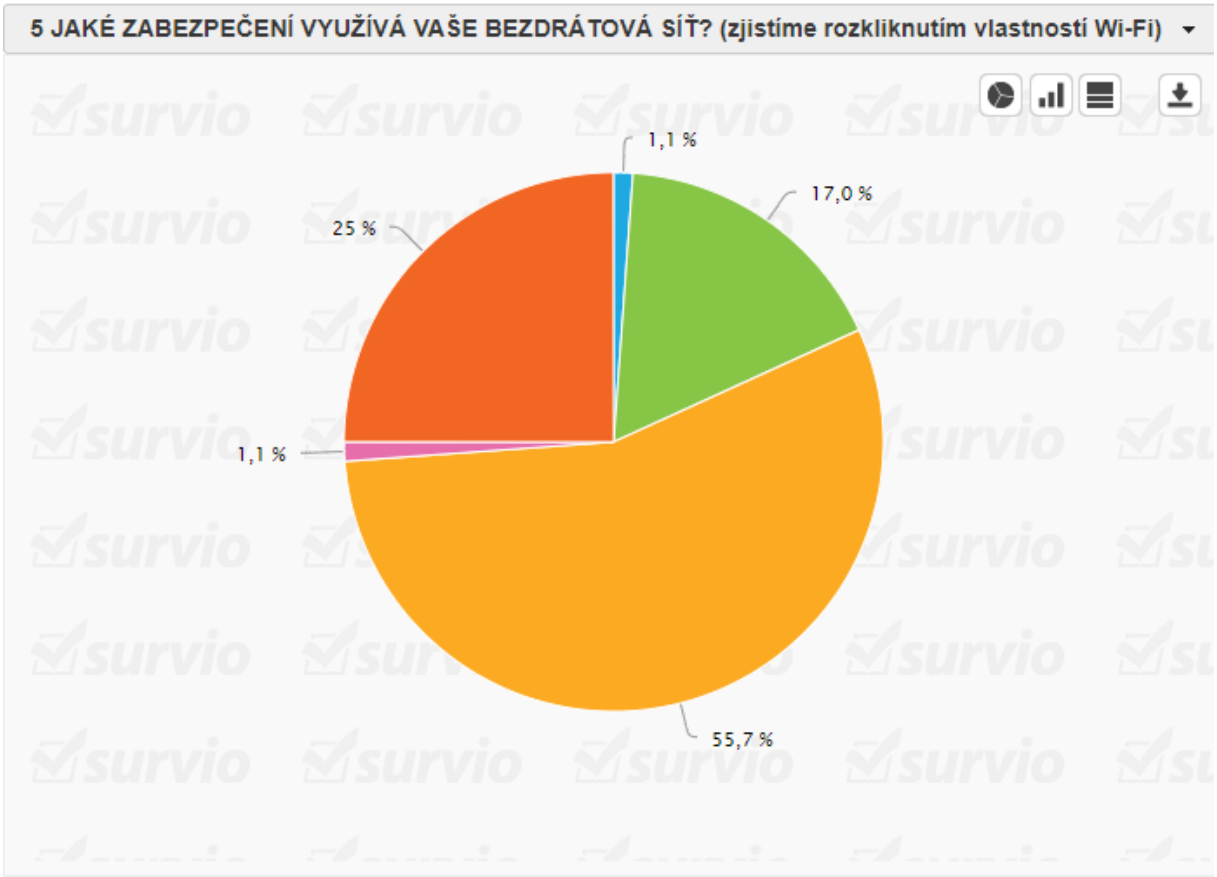
Obr. 13: Síla hesla



Zdroje: AUTOR. Prostřednictvím portálu SURVIO. 2018. Dostupné z: https://www.survio.com/survey/d/S5G7R7C5B7H9L8C9V

Otázka číslo pět se dotazuje na to, jaký typ zabezpečení bezdrátové sítě mají. Navrhl jsem celkově pět možností, z kterých mohou uživatelé vybírat, a to žádné, WEP, WPA, WPA2 a nevím. K této otázce jsem přiložil menší nápovědu, jak tuto informaci zjistit, jelikož někteří uživatelé nejsou tolik znalí v této problematice, aby sami věděli výsledek. I přes to vyplnilo položku „nevím“ 25% respondentů, což dokazuje, že i v dnešní době jsou někteří lidé IT světem nepříliš znalí. Zbylé výsledky můžete posoudit sami v přiloženém obrázku.

Obr. 14: Typy zabezpečení

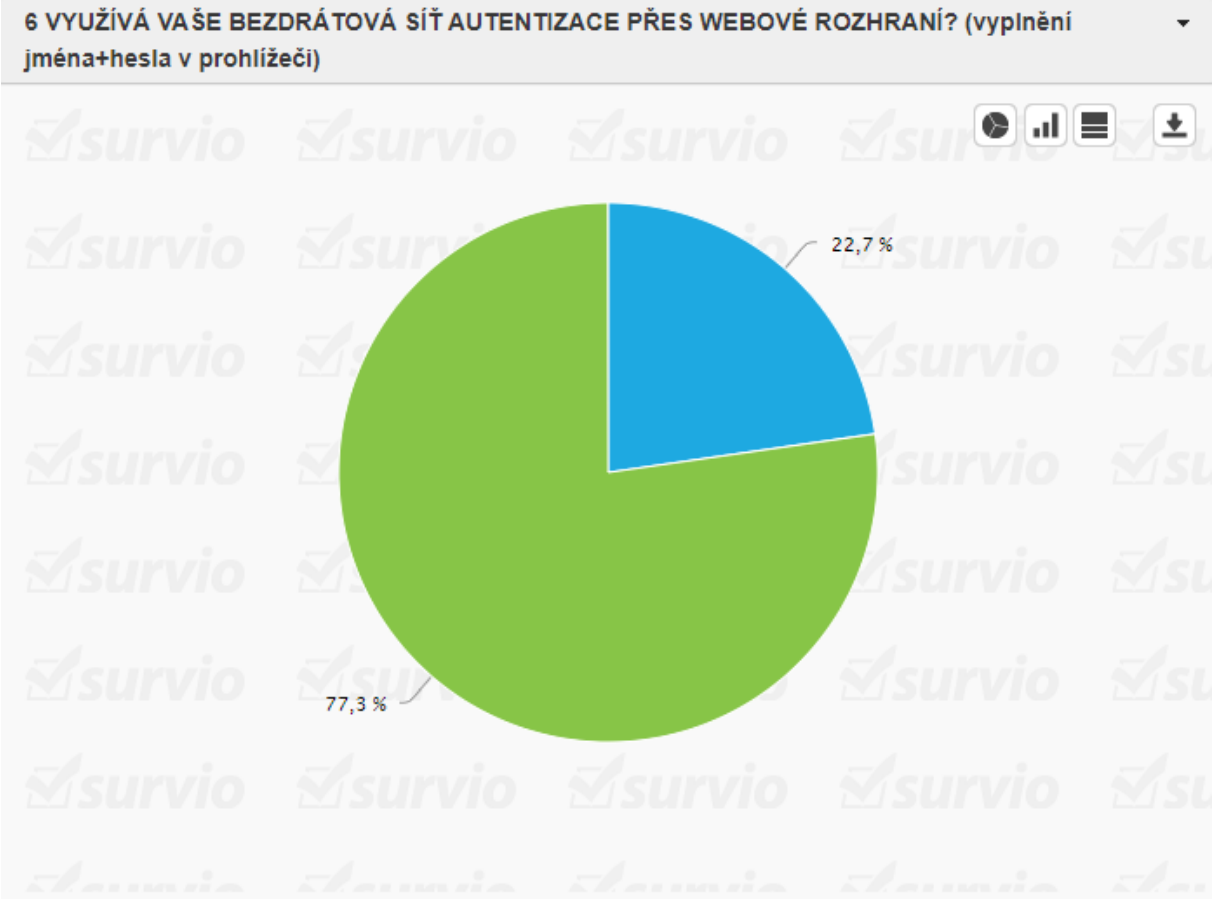


#	Možnosti odpovědí	Responzí	Podíl
●	WEP	1	1,1 %
●	WPA	15	17,0 %
●	WPA2	49	55,7 %
●	ŽÁDNÉ	1	1,1 %
●	NEVÍM	22	25 %

Zdroje: AUTOR. Prostřednictvím portálu SURVIO. 2018. Dostupné z: https://www.survio.com/survey/d/S5G7R7C5B7H9L8C9V

Předposlední otázkou jsem vyzvídal od uživatelů, jestli využívají v přístupu do bezdrátové sítě autentizaci přes webové rozhraní. Tato praktika je velmi využívaná v různých hotelích, penzionech, restauracích či firmách. Analýza této otázky splnila mé očekávání, kdy 22,7% uživatelů uvedlo, že tuto funkci používá.

Obr. 15: Autentizace přes webové rozhraní



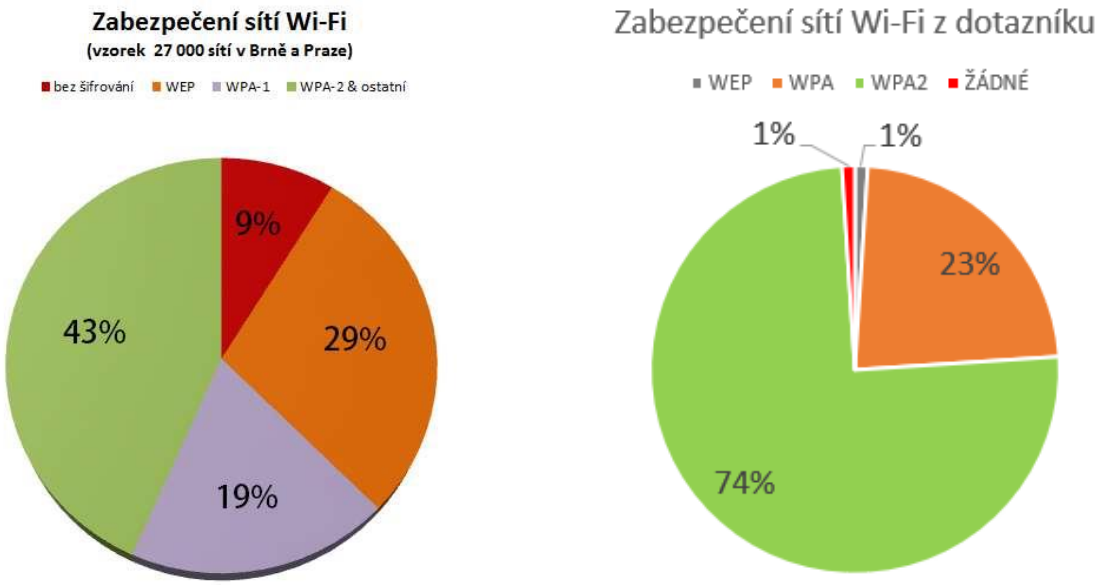
#	Možnosti odpovědí	Responzí	Podíl
●	ANO	20	22,7 %
●	NE	68	77,3 %

Zdroje: AUTOR. Prostřednictvím portálu SURVIO. 2018. Dostupné z: https://www.survio.com/survey/d/S5G7R7C5B7H9L8C9V

Poslední, co jsem ve svém dotazníku uváděl, nebyla přímo otázka, ale spíše takový dotaz, zdali mají respondenti větší zájem o informace týkající se zabezpečení bezdrátové sítě. Celkově osm lidí vyplnilo svůj email, a proto jim po obhajobě tuto práci zašlu, aby dostali veškeré informace, které se bezpečnosti Wi-Fi sítí zabývají.

Celkově bych zde rád shrnul, co vše jsem se z daného dotazníku dozvěděl. Je vidět, že bezdrátovou síť v domácnosti používá téměř každý, což výsledek jasně dokazuje. Využívání Wi-Fi u notebooků, počítačů a mobilních zařízení je běžné, a proto u analýzy vidíme velmi vysoká procenta zastoupení. Velmi mě potěšilo, že téměř všichni mají bezdrátovou síť zaheslovanou, a že ve více než dvou třetinách případů se jedná o silné heslo. Spoustu respondentů odpovědělo, že vlastní typ zabezpečení WPA2, či WPA, což dokazuje, že je dnes brán větší zřetel na bezpečnost sítí. Ve srovnání s výsledky vzorků, který prováděl PC specialista a redaktor počítačového portálu živě.cz roku 2011 a mými výsledky, musím uznat, že se zabezpečení za sedm let opravdu někam posunulo. Pro představu uvádím, jak vypadá graf vzorků prováděný již zmíněným expertem Jakubem Čížkem.

Obr. 16: Zabezpečení sítí Wi-Fi



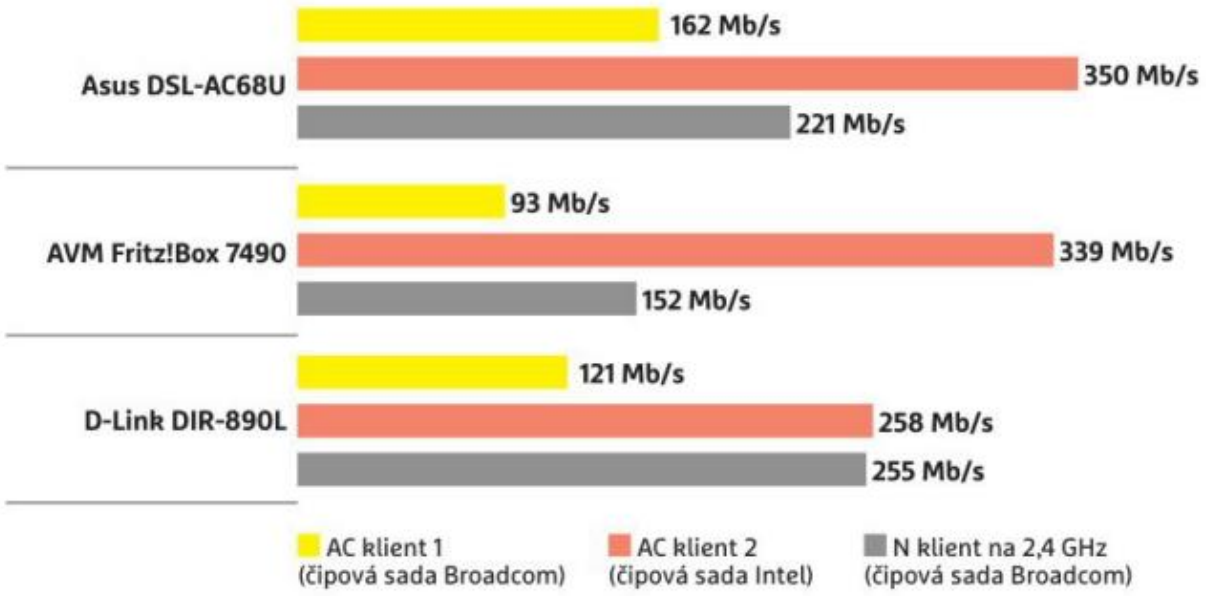
Zdroje: ČÍŽEK. Jakub. Živě. Prolomili jsme se do cizí Wi-Fi sítě [online]. 2011. [cit. 2018-03-28]. Dostupné z: https://www.zive.cz/getthumbnail.aspx?q=60&height=100000&width=100000&id_file=707626822

10 Modelový příklad zabezpečené sítě

Na konec své bakalářské práce bych rád uvedl modelový příklad zabezpečené sítě, aby uživatel přehledně a jednoduše viděl, co vše by měl udělat, aby se nemusel obávat toho, že mu dojde k napadení, odcizení či využití osobních a citlivých dat.

Základním komponentem pro vytvoření bezdrátové sítě, jak již jsme si uváděli v teoretické části práce, je Wi-Fi router. V dnešní době nabízí tyto komponenty spousty společností, mezi které patří například TP-LINK, Tenda, Asus, Zyxel, Cisco a mnohé další. Pouze na českém nejznámějším portálu Alza.cz nabízí k prodeji celkově 170 routerů různých cenových úrovní a různé kvality. Nejlevnější dokážete sehnat za několik set korun, ale nalezneme zde i kousky, které stojí přes deset tisíc. Samozřejmě ceny vycházejí z toho, co vše router dokáže, jaké má v sobě komponenty a mnohé další parametry. Marketing výrobců Wi-Fi routerů ovšem velmi rád přehání. Neexistují totiž žádné oficiální rychlostní kategorie síťových zařízení, podle kterých by se zařízení dělily. Výrobci proto udávají fantastické přenosové rychlosti v Mb/s. Abyste na tyto marketingové triky neskočili, je třeba si uvědomit, že jde jen a pouze o teoretické hodnoty a jejich dosažení je v praxi téměř nemožné. Proto je podle mého názoru daleko lepším měřítkem různá hodnocení od uživatelů, žebříčky top IT firem nebo porovnání v různých medií zabývající se světem technologií. Zde můžete vidět příklad srovnání několika routerů redaktorem jednoho z nejznámějších českých počítačových časopisů CHIP [14].

Obr. 17: Porovnání rychlostí routerů

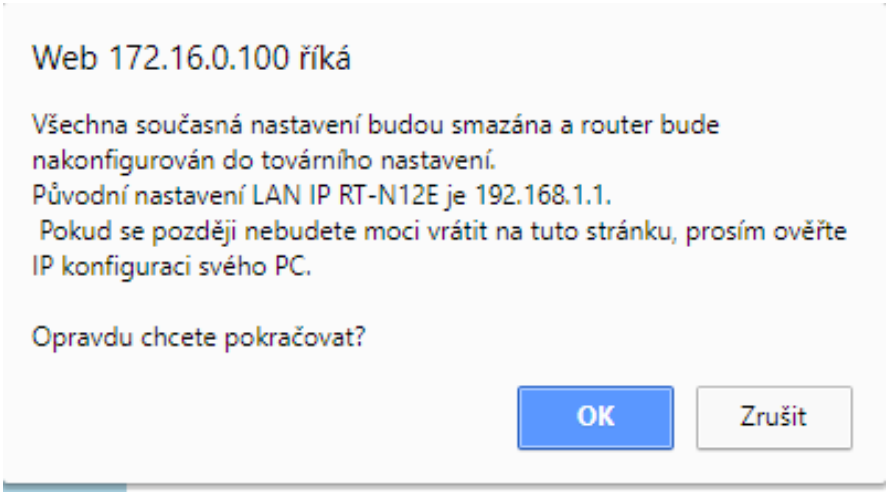


Zdroje: GEIGER, Jörg. Nejrychlejší Wi-Fi routery. Praha: Burda s.r.o. 2016. Počítačový magazín CHIP, ISSN 1210-0684

V mé domácí sítí máme router ASUS RT-N12E. Tento výrobek, jak již poukazuje graf rychlostí routeru, pochází od stejné firmy, která má nejlepší dosažené výsledky. ASUS RT-N12E C1 je router třídy Wireless N s rychlostí 300 Mb/s, který nabízí kabelové i bezdrátové připojení optimalizované speciálně pro malé firmy a domácnosti. Pomocí technologie 2T2R MIMO a dvojice externích antén s vysokým ziskem zajišťuje širší pokrytí a vyšší bezdrátový výkon. Proto je ideální pro streamování HD videa nebo hraní on-line her. Díky intuitivnímu grafickému uživatelskému rozhraní a jedinečné funkci Quick Internet Setup (rychlé nastavení internetu) zvládne RT-N12E C1 nainstalovat a ovládat i naprostý začátečník. Další funkci, kterou router nabízí, je řízení přístupu hostů do sítě. Funkce ASUS Guest Network podporuje až tři samostatné sítě pro hosty, přičemž každá z nich má své vlastní heslo a limity využití. Hosté tudíž nemohou přistupovat k vaší primární síti a ani k jakýmkoli jiným připojeným zařízením [15].

Teď již pojďme k samostatnému nastavení routeru. Pro praktickou ukázku, jak postupovat, musím své zařízení dát do továrního nastavení, abych zde mohl uvést všechny kroky, které má uživatel udělat.

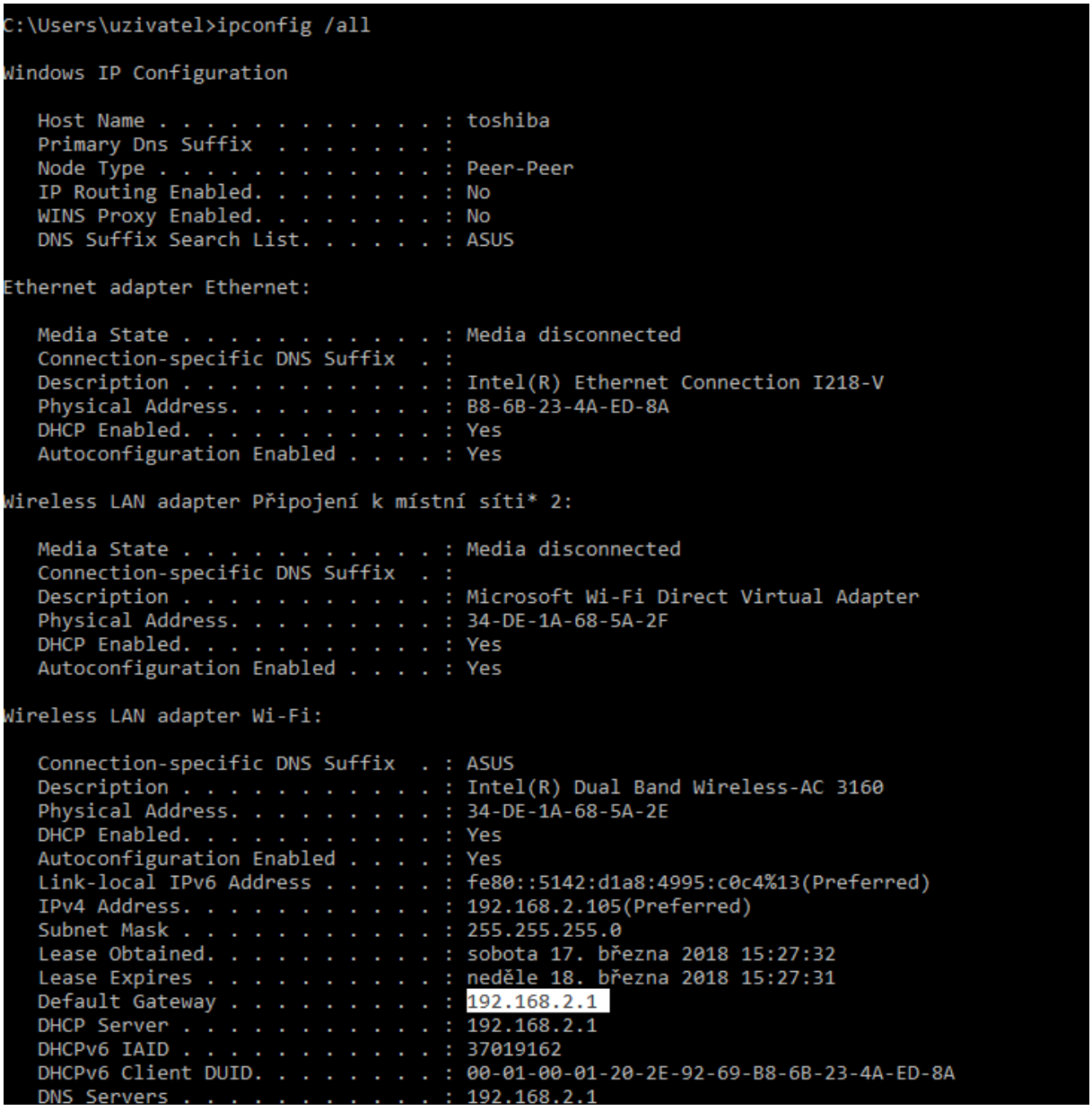
Obr. 18: Tovární nastavení



Zdroje: AUTOR. Screenshot dialogového okna při konfiguraci routeru do továrního nastavení. 2018

První nutností je připojení kabelu od vašeho poskytovatele internetu do WAN portu. Následně se pomocí počítače, notebooku či jiného zařízení připojíme k dané bezdrátové síti a spustíme webový prohlížeč. Po otevření prohlížeče se nám zobrazí většinou dialogové okno, pomocí kterého se po potvrzení připojíme k internetu, jelikož tento router vlastní funkci Quick Internet Setup, který jsem již zmiňoval. Pro ruční nastavení zařízení si musíme najít adresu výchozí brány, pomocí příkazu ipconfig /all v příkazovém řádku.

Obr. 19: Příkazový řádek



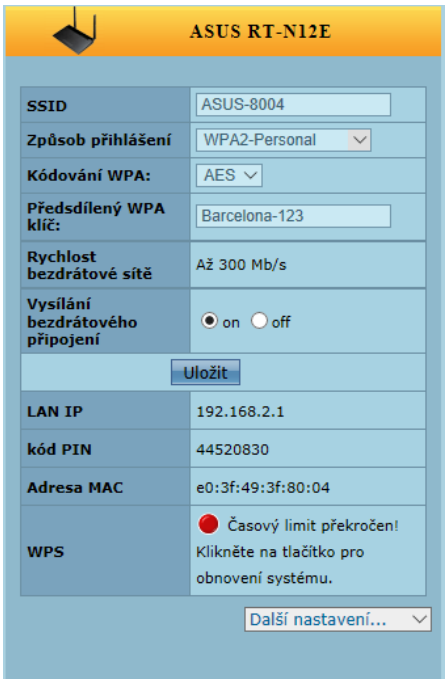
Zdroje: AUTOR. Screenshot využití příkazového řádku. 2018

Co to je příkazový řádek a jak ho mám v počítači otevřít? Příkazový řádek je uživatelské rozhraní, ve kterém uživatel komunikuje s programy nebo operačním systémem pomocí zapisování příkazů. V začátcích se uživatelé při práci s příkazovým řádkem učí pohybovat, přepínat seznamy složek, kopírovat, mazat soubory a tak dále. Profesionálové jsou schopni napsat složité skripty, které při jednom spuštění vykonají hned několik činností najednou. Lidé, kteří se zabývají sítěmi či bezpečností informačních systémů tuto komunikaci často využívají, ať již přes příkazový řádek nebo přes program PuTTY. Je několik možností, jak toto rozhraní zapnout. V systémech Windows 7, 8 či 10 stačí do vyhledávače napsat příkazový řádek či zkratku cmd (Command Prompt). Ve starším operačním systému Windows XP jsme to otevírali přes dialogové okno Spustit, kam jsme napsali rovněž zkratku cmd.

Výchozí adresa brány je v základním nastavení 192.168.1.1, ale můžete si všimnout na obrázku č.19, že v našem případě přidělil server DHCP jinou adresu a to 192.168.2.1. Došlo k tomu kvůli tomu, že v naší domácí síti nemáme pouze router a výchozí adresa je již obsazena.

Tuto adresu 192.168.2.1 zkopírujeme nebo napíšeme do webového prohlížeče a vyplníme jméno „admin“ a heslo „admin“. Dostali jsme se do nastavení routeru a můžeme zde pokračovat a vše správně nastavovat. V kolonce způsob přihlášení nastavíme WPA2 Personal, který nám poté automaticky změní kódování WPA na AES. Do políčka před sdílený WPA klíč vyplníme heslo, které by mělo obsahovat minimálně osm znaků, z toho minimálně jedno velké písmeno, jedno malé písmeno, jedno číslo a jeden nepísemný znak. Důvody jsme si již uváděli v teoretické části mé práce.

Obr. 20: Základní ruční nastavení routeru

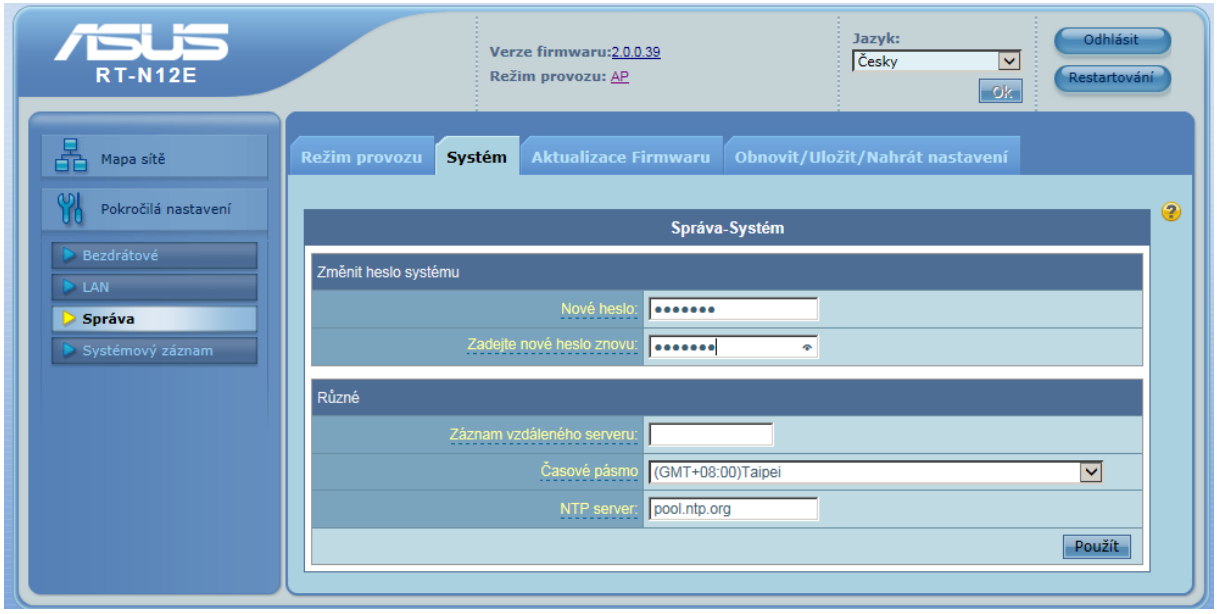


Zdroje: AUTOR. Screenshot z ručního nastavování routeru ASUS RT-12E. 2018

Po zadání hesla ovšem přichází otázka, jak si máme všechny ta hesla pamatovat? Na sociální sítě, do mailů, do bankovnictví, do mobilu a do dalších desítek portálů? Odborníci doporučují program Keepass, který je výborně zabezpečený hlavním heslem a souborem s osobním klíčem. Databáze hesel je šifrovaná pomocí šifer AES nebo Twofish. Zde můžete spravovat všechna svá hesla, která se vám třídí do různých skupin a podskupin podle času vytvoření, času posledního přístupu nebo také podle expirační doby.

Vrátíme se k nastavení routeru. Po rozkliknutí pokročilého nastavení se objeví několik, již v praktické části zmíněných funkcí, mezi které patří například filtrování MAC adres, skrytí SSID nebo také filtrování URL adres a klíčových slov. V pokročilém nastavení můžeme změnit i IP adresu routeru či vidět přidělenou adresu připojených zařízení. Nadstavbou může být vytvoření virtuálního serveru, funkce QoS (zaručuje dosažení požadované rychlostní charakteristiky sítě) a mnohé další, kterými bych ale obyčejné uživatele nezatěžoval. Následně se velmi doporučuje změnit přihlašovací údaje pro správu routeru, které jsou ve výchozím nastavení ve tvaru slova „admin“. Pomocí systémových nástrojů se dostaneme na místo, kde můžeme změnit jméno i heslo na nové. Tyto údaje hlavně nezapomeňte, protože jinak se do správy nedostanete a budete muset ručně obnovovat výchozí výrobní nastavení zařízení.

Obr. 21: Změna přihlašovacích údajů pro správu routeru



Zdroje: AUTOR. Screenshot z ručního nastavování routeru ASUS RT-12E. 2018

11 Závěr

V této práci jsem se zaměřil na analýzu bezdrátových sítí v domácnosti, přičemž jsem kladl velký důraz na seznámení normálního uživatele s nebezpečím, které může hrozit, a na to, jak co nejlépe svoji síť zabezpečit. Jelikož si myslím, že stále existuje spousta jedinců, kteří nejsou s tématikou bezpečnosti moc seznámeni, tak jsem si dal za cíl, to pomocí mé práce napravit. Práci jsem se snažil napsat jednoduše a efektivně tak, aby to pochopil úplně každý.

Prvním cílem bylo v teoretické části seznámit čtenáře s obecnými poznatky o bezdrátových sítích, její výhody a nevýhody a jaké zařízení k správnému fungování potřebujeme. Poté jsem nastínil historii bezdrátových sítí a popsal standardy 802.11. Následně jsem se zabýval již zabezpečením, jejími různými typy a doporučením, které je pro uživatele nejlepší a nejbezpečnější. Věnoval jsem pozornost i heslu, aby čtenáři věděli, jak při volbě hesla správně postupovat. Počítačoví experti doporučují, jak již z mé práce vyplývá, že pro uživatele je nejbezpečnější využívat nejnovější šifrovací protokol WPA2, který je s kombinací silného heslo téměř neprolomitelný. Tento cíl považuji za splněný, jelikož jsem uvedl dané informace tak, abych co nejlépe obeznámil uživatele s danou problematikou.

V další části jsem se rozepsal o kamerových systémech, alarmech a o ovládání topení, které se dnes využívají i bezdrátově, přičemž největší výhodou těchto zařízení je, že již nemusíme vést kabely nutné k jejich funkčnosti. Čtenáři jsem rozšířil vědomosti a znalosti tohoto tématu, a proto i tento cíl plně naplňuji.

Mým dalším cílem bylo přiblížit téma o ochraně dětí na internetu a na počítači, jelikož si myslím, že je to velmi důležité, protože nástrahy čekají na každém kroku. V práci uvádím různé metody a programy, které pomáhají rodičům chránit jejich ratolesti a tuto část práce považuji za úspěšně splněnou.

Pomůckou pro naplnění mého posledního cíle byl dotazník, který obsahoval sedm otázek a který mi po zodpovězení od všech respondentů pomohl lépe diagnostikovat problémy uživatelů. Následně jsem výsledky zabezpečení porovnal s českým expertem Jakubem Čížkem, který se zabýval stejnou tématikou již roku 2011. Ve srovnání můžeme vidět, že se bezpečnost posunula kupředu a že je již dnes na zabezpečení sítí brán větší zřetel.

V praktické části jsem pro dosažení již zmíněného posledního cíle uvedl modelovou situaci zabezpečené sítě, která slouží jako návod pro uživatele, aby věděli, jak mají postupovat, aby docílili ve své domácnosti co nejbezpečnější domácí sítě. Po přečtení mé práce je mnohem jasnější, co vše by měl člověk udělat, a proto jsem rád, že jsem tímto svůj cíl naplnil.

12 Seznam zkratek

Wi-Fi	Wireless Fidelity
IEEE	Institute of Electrical and Electronics Engineers
MHz	Megahertz
USA	United States of America
GSM	Global System for Mobile Communications
LAN	Local Area Network
USB	Universal Serial Bus
GHz	Gigahertz
IT	Informační technologie
Mbit/s	Megabit za sekundu
OFDM	Orthogonal Frequency Division Multiplexing
MAC	Media Access Control
QoS	Quality of Service
IP	Internet Protocol
MIMO	Multiple-input multiple-output
BSS	Base Station Subsystem
ISP	Internet service provider
OSI	Open Systems Interconnection
cmd	Command Prompt
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
SSID	Service Set Identifier
ASCII	American Standard Code for Information Interchange
AP	Access point
ESS	Extended Service Set

CRC	Cyclic redundancy check
VPN	Virtual private network
TKIP	Temporal Key Integrity Protocol
AES	Advanced Encryption Standard
CCMP	Counter Cipher Mode with Block Chaining Message Authentication Code Protocol
KRACK	Key Reinstallation Attacks
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
WPS	Wi-Fi Protected Setup
PIN	Personal identification number
TCP	Transmission Control Protocol
PC	Personal computer
Mb/s	Megabyte za sekundu
HD	High Definition
WAN	Wide Area Network
DHCP	Dynamic Host Configuration Protocol
AES	Advanced Encryption Standard
URL	Uniform Resource Locator

13 Seznam obrázků

14 Seznam tabulek

15 Literatura

[1] SURYNEK, Jiří. Problematika bezdrátových sítí [online]. 2003 [cit. 2018-02-26]. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=31240

[2] VRÁTNÝ, Jan. Audit zabezpečení bezdrátových sítí [online]. 2012 [cit. 2018-02-26]. Dostupné z: https://theses.cz/id/f790lc/Jan_Vrtn_-_bakalsk_prce_2012.pdf

[3] KOLCUN, Jiří. Zabezpečení Wi-Fi sítí [online]. 2010 [cit. 2018-02-26]. Dostupné z: https://is.bivs.cz/th/7128/bivs_b/Bakalarska_prace.pdf

[4] THOMAS, Tom. SSID (Service Set IDentifier) [online]. 2012 [cit. 2018-02-26]. Dostupné z: http://www.tech-faq.com/ssid.html

[5] OU, George. The six dumbest ways to secure a wireless LAN [online]. 2005 [cit. 2018-02-26]. Dostupné z: https://www.zdnet.com/article/the-six-dumbest-ways-to-secure-a-wireless-lan/

[6] NANCY, Cam. Security flaws in 802.11 data link protocols [online]. 2003 [cit. 2018-02-26]. Dostupné z: https://people.eecs.berkeley.edu/~daw/papers/wireless-cacm.pdf

[7] VÁCLAVÍK, Lukáš. Wi-Fi už možná není bezpečné. Šifrování WPA2 prý bylo prolomeno [online]. 2017 [cit. 2018-02-26]. Dostupné z: https://www.cnews.cz/wi-fi-uz-mozna-nebude-bezpecne-sifrovani-wpa2-pry-bylo-prolomeno/

[8] WILMINGTON. Jak zabezpečit bezdrátovou Wi-Fi síť [online]. 2017 [cit. 2018-02-26]. Dostupné z: https://managementmania.com/cs/jak-zabezpecit-bezdratovou-wi-fi-sit

[9] BOHDALOVÁ, Zuzana. Kamery, kamerový systém a zabezpečení domu [online]. 2013 [cit. 2018-02-28]. Dostupné z: http://www.svepomoci.cz/stavba-domu/rozvody-a-instalace/3017-kamery-kamerovy-system-a-zabezpeceni-domu.html

[10] KUČERA, Petr. Hlavní výhody IP kamerových systémů [online]. [cit. 2018-02-28]. Dostupné z: http://www.bois.cz/bois-opava-a-s/kamerove-systemy/hlavni-vyhody-ip-kamerovych-systemu

[11] PULTAR, Jiří. WIFI termostaty topení a termostaty ovládané GSM signálem [online]. [cit. 2018-02-28]. Dostupné z: https://www.az4.cz/wifi-termostaty/

[12] KRAUS, Josef. Nejlepší program pro monitorování webových stránek [online]. 2012 [cit. 2018-03-01]. Dostupné z: https://www.zive.cz/clanky/nejlepsi-program-pro-monitorovani-webovych-stranek/sc-3-a-163051/default.aspx

[13] ŠPULÁK, Ondřej. Chraňte své děti před nástrahami internetu! [online]. 2008 [cit. 2018-03-01]. Dostupné z: https://www.slunecnice.cz/tipy/chrante-sve-deti-pred-nastrahami-internetu/

[14] GEIGER, Jörg. Nejrychlejší Wi-Fi routery. Praha: Burda s.r.o. 2016. Počítačový magazín CHIP, ISSN 1210-0684

[15] ASUSTek Computer Inc., ASUS RT-N12E [online]. 2017 [cit. 2018-03-23]. Dostupné z https://www.asus.com/cz/Networking/RT_N12E_vB/

[16] ŠÍPEK, Petr. Zabezpečení WPS pro Wi-Fi není bezpečné [online]. 2012 [cit. 2018-04-09]. Dostupné z: https://www.cnews.cz/zabezpeceni-wps-pro-wi-fi-neni-bezpecne/

[17] KASÍK, Pavel. Složitá hesla [online]. 2017 [cit. 2018-04-23]. Dostupné z: https://technet.idnes.cz/nist-doporuceni-hesla-jak-zvolit-silne-heslo-fng-/sw_internet.aspx?c=A170815_065054_sw_internet_pka

[18] PAVELKA, Jindřich. Heslo [online]. 2017 [cit. 2018-04-23]. Dostupné z: https://www.hazardni-hry.eu/pravdepodobnost/heslo.html