Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Bezpečnost dat v počítačových sítích

Ian Gec

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Ian Gec

Systémové inženýrství a informatika
Informatika

Název práce

Bezpečnost dat v počítačových sítích

Název anglicky

Data security in computer networks

Cíle práce

Bakalářská práce je tematicky zaměřena na problematiku bezpečnosti dat počítačových sítí s primárním zaměřením na bezdrátové sítě. Cílem práce je analýza dostupných technologií a postupů pro bezpečnost dat v počítačových sítích a následné vypracování optimálního nastavení bezpečnosti dat v síťové infrastruktuře firmy zabývající se vymáháním pohledávek.
Dílčí cíle práce jsou:
- vypracování přehledu technologií bezdrátových sítí,
- vypracování přehledu rizik a bezpečnostních opatření.

Metodika

Metodika řešení problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů. Vlastní práce spočívá v analýza dostupných technologií a postupů pro bezpečnost dat v počítačových sítích se zaměřením na bezdrátové sítě včetně vypracování optimálního nastavení bezpečnosti dat v síťové infrastruktuře malé a střední firmy. Na základě syntézy teoretických poznatků a výsledků praktické části budou formulovány závěry bakalářské práce.

Doporučený rozsah práce

40 – 60 stran textu.

Klíčová slova

Bezpečnost, Wi-Fi, SSID, IEEE 802.11, VPN, šifrování, RSA, WEP, WAP, typy útoků, typy útočníků, MAC adresa, ACL

Doporučené zdroje informací

DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP: Bezpečnost. Brno: Computer Press, 2001. 566 s. ISBN 80-7226-513-X.

NORTHCUTT, Stephen, ZELTSER, Lenny, WINTERS, Scott, FREDERICK, Karen Kent, RITCHEY, Ronald W. Bezpečnost počítačových sítí: Kompletní průvodce návrhem, implementací a údržbou zabezpečené sítě. Brno: Computer Press, 2005. 592 s. ISBN 80-251-0697-7.

SCAMBRAY, Joel, MCCLURE, Stuart, KURTZ, George. Hacking bez tajemství, 2. aktualizované vydání. Brno: Computer Press, 2002. 626 s. ISBN 80-7226-644-6.

SOSINSKY, Barrie A. Mistrovství – počítačové sítě: vše, co potřebujete vědět o správě sítí. Brno: Computer Press, 2010. 840 s. ISBN 978-80-251-3363-7.

ZANDL, Patrick. Bezdrátové sítě WiFi: praktický průvodce. Brno: Computer Press, 2003. 190 s. ISBN 80-7226-632-2.

Předběžný termín obhajoby

2019/20 LS – PEF

Vedoucí práce

Ing. Pavel Šimek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 26. 8. 2019

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 14. 10. 2019

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 15. 02. 2020

Čestné prohlášení

Prohlašuji, že jsem svou bakalářskou práci "**Bezpečnost dat v počítačových sítích**" vypracoval samostatně pod vedením mého vedoucího bakalářské práce pana Ing. Pavla Šimka, Ph.D..

Pro vytvoření této bakalářské práce byla použita odborná literatura a další informační zdroje, které jsou řádně citovány v práci a uvedeny v seznamu použitých zdrojů na samém konci práce.

Jako autor bakalářské práce dále prohlašuji, že jsem v souvislosti s vytvořením této práce neporušil autorská práva třetích osob.

V Praze dne 4.3.2020 .....

Ian Gec

Poděkování

Rád bych poděkoval touto cestou panu Ing. Pavlu Šimkovi, Ph.D. za příkladné vedení mé bakalářské práce, za jeho ochotu a cenné rady při zpracovávání této bakalářské práce. Dále bych rád poděkoval mé rodině za podporu ve vypjatých situacích, které mě během tvorby bakalářské práce potkaly.

Bezpečnost dat v počítačových sítích

Abstrakt

Bakalářská práce je tematicky zaměřena na problematiku bezpečnosti dat počítačových sítí s primárním zaměřením na bezdrátové sítě. Cílem práce je analýza dostupných technologií a postupů pro bezpečnost dat v počítačových sítích a následné vypracování optimálního nastavení bezpečnosti dat v síťové infrastruktuře firmy zabývající se vymáháním pohledávek.

Klíčová slova

Bezpečnost, Wi-Fi, SSID, IEEE 802.11, VPN, šifrování, RSA, WEP, WAP, typy útoků, typy útočníků, MAC adresa, ACL

Data security in computer networks

Abstract

Bachelor thesis is focused on data security of computer networks with primary focus on wireless networks. The goal of the bachelor thesis is to analyze the available technologies and procedures for data security in computer networks and subsequently to develop an optimal data security setting in the network infrastructure of the company dealing with debt collection.

Keywords

Security, Wi-Fi, SSID, IEEE 802.11, VPN, encryption, RSA, WEP, WAP, types of attacks, types of attackers, MAC address, ACL

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

V moderní době je již téměř nepředstavitelné, že by člověk bez internetu mohl existovat. Tato technologie se prokazatelně začlenila do života většiny lidí v civilizované společnosti. Internet se integroval do volného času, v práci či ve škole. Standardní vybavení člověka je např. mobilní telefon, tablet, chytré hodinky, počítač či notebook, které mají přístup na internet ať už pomocí drátového nebo bezdrátového připojení. Je to díky dostupnosti zařízení, ceně a samozřejmě snadnému přenosu těchto zařízení.

Postupem času se masivně rozmáhají mobilní zařízení a smart technologie, která jsou připojena pomocí Wi-Fi připojením. Data jsou zde přenášena např. vzduchem nebo vakuem za pomoci elektromagnetického vlnění. Tím se samozřejmě zvyšuje riziko odcizení dat či přebrání kontroly nad zařízením. Díky tomu se musí agilně zvyšovat ochrana dat a zařízení v celé síťové infrastruktuře, protože i malá neopatrnost člověka či bezpečnostní chyba na zařízení nebo aplikaci může mít pro oběť finanční či existenční dopad.

Wi-Fi sítě mají své základní výhody a nevýhody. Výhoda bezdrátové sítě je její cena a možnost dálkového bezdrátového přenosu dat, ale jen do omezené vzdálenosti vysílače od přijímače. Hlavní nevýhoda bezdrátové sítě je omezená přenosová rychlost naproti drátovému připojení a možnosti vytvoření, tzv. Free Wi-Fi, která může sloužit jako zadní vrátka hackerům do připojených zařízení.

Útoky hackerů se již nezaměřují jen na firmy, ale i na jednotlivce, protože převážně mladí lidé a lidé v produktivním věku používají ve svých mobilních zařízeních internetové bankovnictví, z kterého je hacker schopen odcizit finanční prostředky ve svůj prospěch.

2 Cíl a metodika práce

2.1 Cíl práce

Bakalářská práce je tematicky zaměřena na problematiku bezpečnosti dat počítačových sítí s primárním zaměřením na bezdrátové sítě. Cílem práce je analýza dostupných technologií a postupů pro bezpečnost dat v počítačových sítích a následné vypracování optimálního nastavení bezpečnosti dat v síťové infrastruktuře firmy zabývající se vymáháním pohledávek.

Dílčí cíle práce jsou:

- vypracování přehledu technologií bezdrátových sítí
- vypracování přehledu rizik a bezpečnostních opatření

2.2 Metodika práce

Metodika problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů a dostupných zdrojů online. Teoretická část bakalářské práce spočívá v analýze dostupných technologií a postupů pro bezpečnost dat v počítačových sítích se zaměřením na různé technologie bezdrátových sítí, Wi-Fi protokoly, přehled rizik a přehled bezpečnostních opatření.

Praktická část bakalářské práce bude zpracována dle získaných poznatků z teoretické části práce a osobních znalostí získaných ze zaměstnání a během studia. Tato část bude zpracována jako analýza s následnou implementací výsledků do optimálního nastavení zabezpečení infrastruktury sítě malého podniku. Pro analýzu bude použita vícekriteriální analýza variant, přesněji metoda pořadí se stanovenými váhami.

Na základě syntézy teoretických poznatků a výsledků praktické části budou formulovány závěry bakalářské práce.

3 Teoretická východiska

Teoretická část bakalářské práce popisuje typy Wi-Fi sítí, jejich historický vývoj, Wi-Fi standardy, režimy provozu, šifrování dat, druhy šifrování, možné útočníky, možné útoky, rizika, která právě provozování Wi-Fi sítí přináší a druhy zabezpečení, který právě tato rizika se snaží eliminovat.

3.1 Počítačová síť

Počítačová síť je spojení dvou a více zařízení (síťových uzlů), které společně mohou komunikovat či sdílet různé prostředky. Data se v počítačové síti přenášejí pomocí připojení drátového, bezdrátového nebo jejich vzájemnou kombinací. Každé zařízení v počítačové síti má svojí MAC adresu, což je jednoznačný identifikátor síťového zařízení, který má velikost 48 bitů. [7]

3.2 Bezdrátová síť

Bezdrátová síť je síť, kde se data přenáší prostředím do různých vzdáleností bez nutnosti klasické kabelového připojení pro přístup do systému internet. Vzdálenosti, ve kterých data mohou být ještě zpracována, jsou ovlivněny rozmístěním komunikujících prvků, frekvencí, rušením, anebo zda jsou prvky ve vnitřním či vnějším prostředí. Bezdrátové sítě se běžně používají tam, kde drátová síť není možná sestrojit ať už z finančního nebo pozičního hlediska. [5]

3.2.1 Dělení bezdrátových sítí

Bezdrátové sítě lze dělit dle různých kritérií. Nejzákladnější dělením je dle závislosti na vzdálenosti klienta od přístupového bodu k internetu. Je to také hlavní kritérium této technologie, které se snaží normalizovat institut IEEE (Institute of Electrical and Electronics Engineers). [4]

Bezdrátové soukromé sítě WPAN (Wireless Personal Area Network)

Tato kategorie zahrnuje datové technologie pro sítě s velmi malým dosahem (přibližně do deseti metrů). Technologie umožňuje uživateli bezdrátové připojení k internetu, avšak dané připojení prakticky funguje jen v jedné místnosti. Hlavní využití této kategorie je propojení různých zařízení mezi sebou tzn. v režimu ad-hoc. Režim ad-hoc nám značí, že zařízení komunikují mezi sebou bez nějakého mezičlánku. Do této kategorie především spadají technologie WANET, Bluetooth, IrDA, Zigbee a další. WPAN je normalizována institutem IEEE ve standardu pod číslem 802.15. [8]

Bezdrátové místní sítě WLAN (Wireless Local Area Network)

Hlavním zástupcem WLAN je Wi-Fi, což je standard dle IEEE 802.11, který popisuje bezdrátovou komunikaci v lokálních sítích. Data v rámci WLAN sítě jsou přenášena pomocí aktivního prvku routeru (směrovače), kde se datagramy, které obsahují data, odesílají pomocí procesu routování (směrování). Router nám slouží jako mezičlánek mezi dvěma sítěmi, kde se skrze něj přenáší data. Je to i hlavní přístupový bod do internetu ve WLAN sítích. Dosah signálu, který router v bezdrátové síti emituje, je nejvíce ovlivněn jeho umístěním a překážkami, které se nacházejí v prostředí (např. silné zdi, další elektronické přístroje pracující na stejné frekvenci atd.). [5]

Bezdrátové metropolitní sítě WMAN (Wireless Metropolitan Area Network)

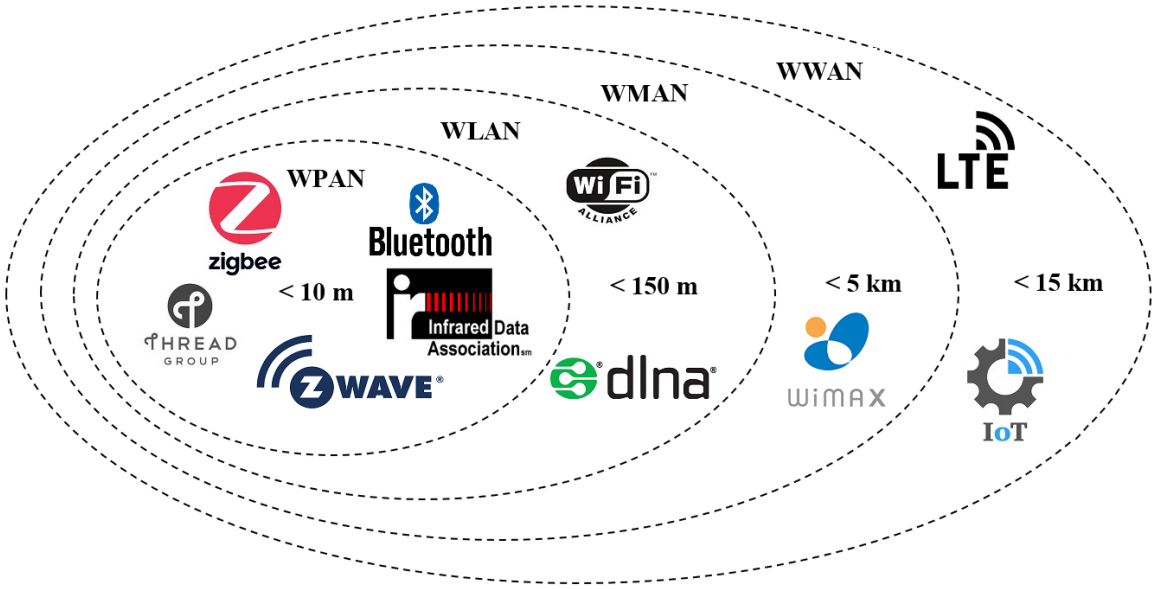
Jedná se o bezdrátový širokopásmový přenos dat v oblasti, která je nějakým způsobem zastavěna (např. města, vesnice, osady) a může se rozpínat až do vzdálenosti 50 km. WMAN síť je hlavně zastoupena technologií WiMax. Standard WMAN je označen jako IEEE 802.26 a je normalizován institutem IEEE. Tento standard specifikuje, že pro přenos dat není nutná přímá viditelnost mezi komunikujícími stranami. [9]

Bezdrátové rozsáhlé sítě WWAN (Wireless Wide Area Network)

Do sítí typu WWAN převážně spadají mobilní telekomunikační technologie neboli mobilní sítě. Mobilní sítě mají velmi rozsáhlé pokrytí a infrastrukturu, hlavně díky komerčnímu využití (volání, SMS, internet). Nejvíce používaný standard je 4G LTE, který měl v České republice skoro 90% pokrytí v roce 2018. [11] V roce 2019 se do komerčního provozu dostala 5G síť, která bude nabízet rychlost internetu až 10 Gbit/s (1,25 GB/s) s velmi nízkou latencí. 5G síť nám umožní nové nepředstavitelné možnosti využití internetu v IoT, virtuální realitě, robotice, 3D 8K přenosy videí, holografické telefonáty a další. [12] Panují zdravotní a bezpečnostní obavy se zavádění 5G sítí tzn. masivní používání vysokých frekvencí, které mohou mít velice negativní dopad na život, jak ho známe, a snadnější sledování lidí. [13]

Typ mobilní sítě	Rychlost stahování dat	Latence
3G LTE	384 Kbit/s	60 ms
4G LTE	100 Mbit/s	50 ms
5G LTE	10 Gbit/s i více	1 ms

Tabulka 1 – Srovnání LTE technologií, zdroj: https://5g.co.uk/guides/how-fast-is-5g/



Obrázek 1 – Bezdrátové sítě a jejich zástupci, zdroj: vlastní zpracování (zdroje značek – internet)

3.3 Wi-Fi

Standard Wi-Fi (Wireless Fidelity) byl vytvořen jako náhrada klasické drátové komunikace se snahou ušetřit finanční prostředky za kabeláž, zpřístupnit větší mobilitu různých zařízeních, vyřešit obtížné instalace kabeláží a nabízet větší volnost při zavádění nových sítích. Tento typ sítě se vyskytuje primárně v domácnostech, ale i ve všech možných institucích jako jsou nemocnice, školy, restaurace, nádraží, a dokonce i ve vybraných dopravních prostředkách MHD. Pro přenos dat se využívá elektromagnetické vlnění v bezlicenčním pásmu kmitočtů, tzv. pásmo ISM. Daná bezlicenční pásma mají svá pravidla a omezení, která stanovuje Český telekomunikační úřad. [4][10]

Wi-Fi síť může být tvořena jako „hotspot“, což je přístupový bod, který bude vyžadovat nějaké ověření (např. certifikát nebo uživatelské jméno a heslo) po zařízení k přístupu k internetu. Další možnost je „free hotspot“, což je přístupový bod, který nebude vyžadovat po zařízení žádnou autentizaci a zařízení poté může komunikovat do internetu. Tento typ připojení se často zneužívá k napadení připojených zařízení.

Technologie Wi-Fi je využívána i poskytovateli internetu (ISP – Internet Service Provider), kteří svým uživatelům standardně nabízejí k tarifům možnost připojení se na Wi-Fi i mimo svůj domov. Toto připojení je umožněno pomocí různých zařízení (routery, modemy) poskytovatele internetu po zadání specifického jména a hesla, které je dodáno poskytovatel internetu. [8]

3.3.1 Historie Wi-Fi

V této a další kapitole budeme mluvit jen o Wi-Fi technologiích, které pracují na frekvenci 2,4 GHz anebo 5GHz.

Vývoj Wi-Fi technologie začal již v září roku 1990, ale teprve v červnu 1997 byl oficiálně vydán první standard IEEE 802.11 Institutem pro elektrotechnické a elektronické inženýrství (IEEE). Přenosová rychlost prvního standardu byla maximálně 2 Mbit/s (pro příklad Ethernet 10 Mbit/s), též vzdálenost přenosu nebyla příliš velká. Data se přenášela za pomoci modulace FHSS (Frequency Hopping Spread Spectrum), která je založena na přeskocích mezi frekvencemi. Jedno Wi-Fi zařízení bylo tedy schopno zabrat celé frekvenční pásmo 2,4 GHz (přesně 2,4 – 2,4835 GHz).

Důsledek toho byl, že s rostoucím počtem zařízení se zhoršovala kvalita komunikace, protože docházelo k častějším kolizím přenosu. Jako prevence byla vytvořena pokročilá modulace OFDM (Orthogonal Frequency Division Multiplexing), kde je frekvenční pásmo 2,4 GHz rozděleno na 13 oddělených kanálů. Tato modulační metoda používá více nosných kmitočtů, kterou jsou dále modulovány podle potřeby různými modulacemi (BPSK, QPSK, 1024 QAM a další) [16]. Nejaktuálnější ekvivalent modulace OFDM je modulace OFDMA (Orthogonal Frequency Division Multiple Access), která se používá u nejmodernějších Wi-Fi standardů (např. v IEEE 802.11ax). [14]

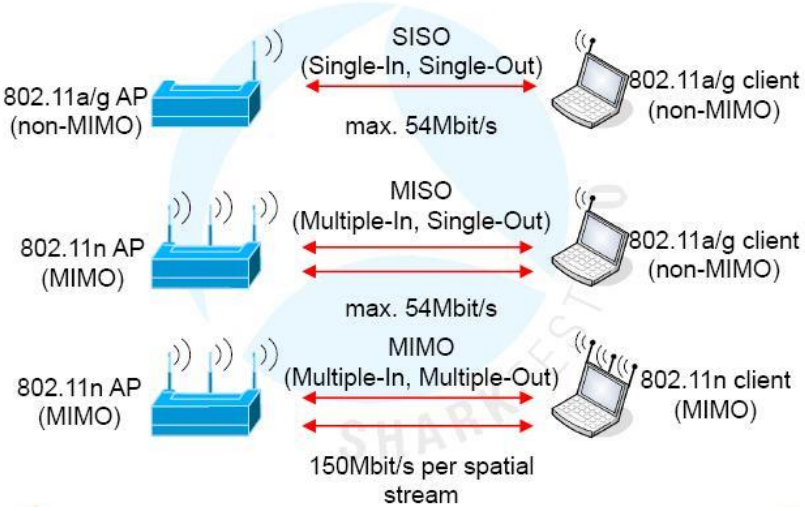
V roce 1999 došlo ke vzniku dvou dalších standardů IEEE 802.11a a IEEE 802.11b. Standard IEEE 802.11a nám přinesl použití frekvence 5,4 GHz (přesně 5,470 – 5,725 GHz). Pásmo 5,4 GHz masivně zlepšilo propustnost až na 54 Mbit/s. Druhý zmíněný standard IEEE 802.11b přinesl pouze přenosovou rychlost 11 Mbit/s v pásmu 2,4 GHz, ale zařízení byla nesrovnatelně levnější než zařízení s IEEE 802.11a.

Analytická firma Gartner v roce 2002 předpověděla, že v roce 2003 dojde k velkému rozvoji Wi-Fi technologií. A skutečně se tak stalo. Tato technologie začala zlevňovat a byl představen nový standard 802.11g, který nabízel přenosovou rychlost dat 54 Mbit/s v pásmu 2,4 GHz. [14]

V mezidobí roků 2003-2010 docházelo ke zvýšenému rozvoji Wi-Fi zařízení ze strany výrobců za požadavkem vyšší přenosové rychlosti. To mělo za následek vzájemné nekompatibility Wi-Fi zařízení od různých výrobců.

Roku 2009 byl vytvořen nový standard IEEE 802.11n, který byl však veřejnosti představen až v roce 2011. Standard navýšil přenosovou rychlost na 150 Mbit/s, ale mohl dosahovat až rychlosti 600 Mbit/s dle specifického nastavení. Jako první standard zavedl

podporu MIMO (Multiple-Input and Multiple-Output) pomocí antén (přijímače a vysílače), což přineslo nárůst datové propustnosti a dosahu při zachování šířky pásma. [14]



Obrázek 2 – MIMO technologie u Wi-Fi, zdroj: http://2.bp.blogspot.com/-YWlUjtCCuGY/UBst1DgYahI/AAAAAAAAAc0/TXDOKRZovL0/s1600/MIMO_1.JPG

Rok 2013 přinesl standard IEEE 802.11ac, jež prolomil hranici a zvýšil teoretickou datovou propustnost až na 1,8 Gbit/s.

Na konci roku 2019 byl schválen standard 802.11ax, který je označován jako Wi-Fi 6 a přináší teoretickou datovou propustnost až do 11 Gbit/s.

3.4 Standard IEEE 802.11

Výraz IEEE 802.11 označuje standard pro bezdrátové sítě, který neobsahuje doplňky. Pracuje v pásmu 2,4 GHz při maximální rychlosti 2 Mbit/s. Standard je vyvinut a vyvíjen 11. pracovní skupinou IEEE LAN/MAN standardizační komise (IEEE 802). Díky nedostatečné rychlosti a zabezpečení přenosu dat je standard upravován pomocí doplňků, které nedostatky upravují. Množina doplňků je označována jako 802.11x, kde se za x dosazuje písmeno abecedy, které je zrovna v pořadí. [5][15]

Přehled Wi-Fi standardů IEEE 802.11					
Standard	Obchodní označení	Rok vydání	Pásmo [GHz]	Maximální rychlost [Mbit/s]	Fyzická vrstva
IEEE 802.11	Nemá	1997	2,4	2	DSSS, FHSS
IEEE 802.11a	Wi-Fi 1	1999	5	54	OFDM
IEEE 802.11b	Wi-Fi 2	1999	2,4	11	CCK, DSSS
IEEE 802.11g	Wi-Fi 3	2003	2,4	54	DSSS, OFDM
IEEE 802.11n	Wi-Fi 4	2009	2,4 nebo 5	600	MIMO OFDM
IEEE 802.11ac	Wi-Fi 5	2013	5	1 800	MU-MIMO OFDM
IEEE 802.11ax	Wi-Fi 6	2019	1 až 7	10 530	MU-MIMO OFDMA

Tabulka 2 – Přehled Wi-Fi standardů IEEE 802.11, zdroj: http://wi-fi.unas.cz/ieee-802-11.php

3.4.1 IEEE 802.11a - (Wi-Fi 1)

Standard IEEE 802.11a na rozdíl od IEEE 802.11 pracuje v pásmu 5 GHz a přináší přenosovou rychlost až do 54 Mbit/s, což je výrazně vyšší než původní standard. Pro dosažení této rychlosti se poprvé v paketových komunikacích začal používat pokročilý způsob modulace OFDM. Tato modulace se dosud používala jen u systému DAB (Digital Audio Broadcasting) nebo DVB (Digital Video Broadcasting) určených pro distribuci digitálního zvuku a videa.

Hlavní výhoda IEEE 802.11a naproti IEEE 802.11 není jen vyšší rychlost, ale i použitý kmitočet. Kmitočtové pásmo 5 GHz je méně vytížené než pásmo 2,4 GHz, a tedy dovoluje využití více kanálů bez vzájemného rušení. IEEE 802.11a nabízí až osm vzájemně nezávislých a nepřekrývajících se kanálů. [1][17]

Nevýhoda vyššího kmitočtového pásma je, že signál hůře proniká stěnami a jinými překážkami, které se nacházejí v prostředí. [18]

3.4.2 IEEE 802.11b - (Wi-Fi 2)

Standard IEEE 802.11b poskytuje přenosovou rychlost až do 11 Mbit/s v pásmu 2,4 GHz. Pro její dosažení se používá nový způsob kódování, tzv. CKK (Complementary Code Keying) s použitím DSSS (Direct Sequence Spread Spectrum) na fyzické vrstvě. Tento standard byl ve své době velmi populární, hlavně díky nízké pořizovací ceně. [17]

Nevýhoda toho standardu však je, že pracuje v neregulovaném frekvenčním pásmu, a díky tomu může být přenos negativně ovlivňován, tzv. rušen. Proto standard specifikuje, že podle momentálního rušení v prostředí se dynamicky mění rychlost přenosu na 11 Mbit/s (CCK), 5,5 Mbit/s (CCK), 2 Mbit/s (DQPSK) nebo jen 1 Mbit/s (DBPSK). [1][17][18]

3.4.3 IEEE 802.11g - (Wi-Fi 3)

Standard IEEE 802.11b poskytuje vysokou rychlost přenosu dat a udržuje zpětnou kompatibilitu s produkty 802.11b, protože oba standardy pracují na stejném radiovém pásmu 2,4 GHz. Pro dosažení přenosové rychlosti až 54 Mbit/s se používá na fyzické vrstvě OFDM. Pro zpětnou kompatibilitu s IEEE 802.11b se používá DSSS.

Tento standard opět trpí stejnou interferencí jako IEEE 802.11b v již přeplněném pásmu 2,4 GHz, ale lze tomu částečně zabránit umístěním zařízení IEEE 802.11g v rozumné vzdálenosti od jiných zařízení. Pro modulaci se dle hodnoty rušení používají QPSK, BPSK, 16-QAM či 64-QAM. Podporované rychlosti dle modulace jsou následující: 54 Mbit/s (64-QAM), 48, 36 a 24 Mbit/s (16-QAM), 18 a 12 Mbit/s (QPSK), 9 a 6 Mbit/s (BPSK). Další rychlosti jsou stejné jako u IEEE 802.11b. Poskytuje též lepší funkce zabezpečení jako jsou

například ověřování WAP (WiFi Protected Access) a WPA2 s předem sdíleným klíčem nebo serverem RADIUS. [17][18]

3.4.4 IEEE 802.11n - (Wi-Fi 4)

Standard IEEE 802.11n upravuje různé možnosti nastavení parametrů fyzické vrstvy a MAC (Media Access Control) podvrstvy pro zvýšení datové propustnosti až na 600 Mbit/s. Mezi tyto možnosti patří použití více antén (MIMO) jako přijímače a vysílače, změny kódovacích schémat, širší RF pásmo a změny MAC protokolů. Kromě toho může IEEE 802.11n pracovat v pásmu 2,4 GHz nebo 5 GHz a je zpětně kompatibilní s produkty IEEE 802.11a v pásmu 5 GHz, IEEE 802.11b a IEEE 802.11g v pásmu 2,4 GHz. [17][18]

3.4.5 IEEE 802.11ac - (Wi-Fi 5)

Standard IEEE 801.11ac může poskytovat přenosovou rychlost přes 1 Gbit/s (až 1,8 Gbit/s), a tak se také nazývá Gigabit Wi-Fi. Toho je dosaženo rozšířením a vylepšením konceptů zavedených standardem IEEE 802.11n – širší pásmo RF, více MIMO prostorových kanálů, víceuživatelské MIMO pro downlink a modulaci 256-QAM s vysokou hustotou. IEEE 801.11ac funguje pouze v pásmu 5 GHz, ale je stále zpětně kompatibilní s bezdrátovými standardy IEEE 802.11n, IEEE 802.11g, IEEE 802.11b a IEEE 802.11a. [18]

3.4.6 IEEE 802.11ax - (Wi-Fi 6)

Standard IEEE 802.11ax je charakterizován podporou přenosové rychlosti až do 10 Gb/s. Dosáhnutí této rychlosti je právě možné pomocí kombinace přenosu dat mezi Wi-Fi pásmy 2,4 a 5 GHz. Tento standard však hned od svého začátku je schopen podporovat přenosová pásma od 1 GHz až do pásma 7 GHz. Standard se orientuje na vysoký počet klientů a jejich hustotu, což bude mít za následek rozmach smart a IoT technologií.

Pro zlepšení efektivního využití přenosového pásma se zavedla lepší metoda řízení výkonu, aby se zabránilo interferenci se sousedními sítěmi – OFDMA. Dále výkonnější metoda modulace 1024-QAM a MU-MIMO (Multiple-User Multiple-Input and Multiple-Output) pro další zvýšení propustnosti a výkonu. Nově i podpora nového standardu šifrování zabezpečení WPA3. Nabízí vyšší úroveň zabezpečení ve srovnání s původním standardem WPA2 a zlepšení v oblasti spotřeby energie (Target Wake Time).

IEEE 802.11ax vytváří širší kanály a tyto kanály poté rozděluje do menších dílčích kanálů. Díky tomu je k dispozici mnohem více dostupných kanálů, což pro koncové body zefektivňuje a maximálně zjednodušuje cestu k přístupovým bodům. Standard IEEE 802.11ax je zpětné kompatibilní s IEEE 802.11ac a IEEE 802.11n. [19]

3.5 Režimy provozu Wi-Fi

Režimy provozu Wi-Fi sítí nám umožnují vzájemně propojit dvě a více síťových zařízení. Daná zařízení mohou spolu komunikovat na přímo v režimu Ad-hoc anebo nepřímo v režimu infrastruktury. Při nepřímé komunikace se používá prostředník, tzv. přístupový bod (Access Point – AP). Přes přístupový bod je poté vedena všechna síťová komunikace, která je prováděna v dané síti mezi zařízeními.

3.5.1 Režim Ad-hoc

V režimu ad-hoc (ad-hoc mode) Wi-Fi sítě jsou navzájem propojená síťová zařízení, která jsou v rovnocenné pozici P2P (peer-to-peer). Sítě v tomto režimu nevyžadují centralizovaný přístupový bod. Vzájemná identifikace probíhá pomocí SSID (Service Set Identifier). Propojená zařízení musí být v přímém radiovém dosahu do několika metrů od sebe. [4]

Výhoda Wi-Fi sítě v ad-hoc režimu je, že vyžaduje minimální konfiguraci a lze ji velmi rychle vytvořit. Používá se tedy tam, kde potřebujeme sestavit malou, obvykle dočasnou, levnou bezdrátovou síť nebo jako dočasný nouzový mechanismus, pokud dojde k selhání přístupového bodu.

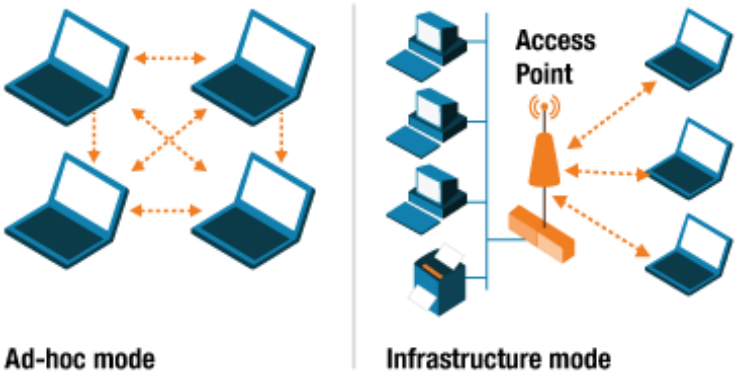
Režim ad-hoc má i své nevýhody. Vyžaduje více systémových prostředků, protože fyzické rozložení sítě se bude měnit s pohybem zařízení. Pokud je k síti ad-hoc připojeno mnoho zařízení, bude vznikat více bezdrátového rušení. Každé zařízení musí tedy navázat přímé spojení s každým jiným zařízením než procházet jediným přístupovým bodem. Předávání dat několika zařízení je však pomalejší než předávání dat jedním bodem. [20]

3.5.2 Režim infrastruktury

V případě bezdrátové sítě v režimu infrastruktura (infrastructure mode) připojujeme zařízení pomocí centrálního zařízení, konkrétně bezdrátového přístupového bodu. Pokud se chceme připojit k síti WLAN, musí být AP a všichni bezdrátoví klienti nakonfigurováni pro použití stejného SSID. Poté je přístupový bod propojen s kabelovou sítí a umožňuje bezdrátovým klientům přístup například k internetovým připojením nebo ke sdíleným periferiím. K síti WLAN lze přidat další přístupové body, aby se zvýšil dosah infrastruktury a podporoval jakýkoliv počet bezdrátových klientů. [4]

Výhoda Wi-Fi sítě v režimu infrastruktury je škálovatelnost, centralizovaná správa zabezpečení a lepší dosah signálu pro přenos dat. Nevýhodou jsou jednoduše dodatečné

náklady na nákup infrastrukturního hardwaru a software pro provoz sítě. [21]



Obrázek 3 – Režimy provozu Wi-Fi: Ad-hoc a Infrastruktury, zdroj: https://files1.element14.com/community/themes/images/2018/wirelesspro2_diagram3.png

3.6 Útoky a rizika

Data, která jsou přenášena pomocí počítačové sítě, mohou být nějakým způsobem odcizena, modifikována či smazána. Na světě neexistuje neprolomitelná pevná počítačová síť, co se týče bezpečnosti a bezdrátové sítě nejsou žádnou výjimkou.

Bezdrátové sítě jsou často zneužívány pro napadení připojených zařízení, kde při útoku slouží jako zadní vrátka. Při nedostatečném zabezpečení bezdrátové sítě se síť může stát obětí útoku zvenčí, ale i zevnitř dané sítě. Síťová komunikace v bezdrátové síti je šířena pomocí radiových vln, které jsou volně šířeny do prostoru v okolí vysílače a díky tomu je tato komunikace lehce zachytitelná, pokud není šifrována. [2]

3.6.1 Cizí bezdrátové zařízení v síti

Bezdrátové zařízení nebo přístupový bod, který je podvodně přidán do sítě a není pod správou síťových administrátorů. Slouží potenciálním útočníkům jako brána do sítě. Tento druh zařízení může být nebezpečně nainstalován, pokud má útočník přímý přístup k pevné síti, ale častěji je přidáváno personálem, který si není vědom důsledků. [3]

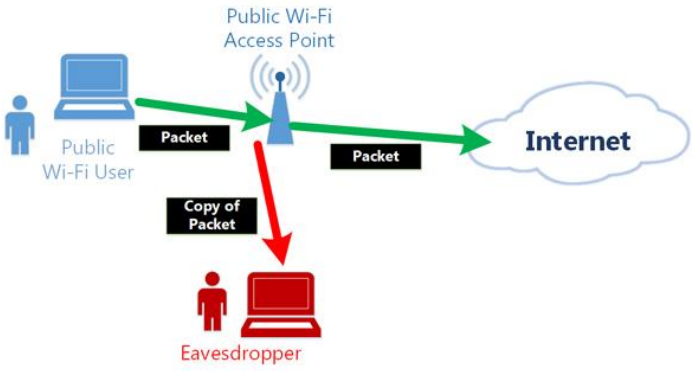
3.6.2 Útoky typu peer-to-peer

Zařízení připojená ke stejným přístupovým bodům mohou být zranitelná vůči útokům jiných zařízení připojených k tomuto přístupovému bodu. Většina poskytovatelů poskytuje možnost, jako je „izolace klientů“, která zajišťuje, že klienti připojeni k přístupovému bodu nemohou spolu komunikovat, což tomuto problému zabraňuje. [3]

3.6.3 Odposlech

Útočník se zaměřuje na probíhající síťovou komunikaci, například mezi uživatelem a jeho bankou pomocí internetového bankovnictví. Při tomto útoku může útočník vystupovat

ve dvou rolích, buď jako pasivní odposlouchávající síťové komunikace, nebo jako aktivní účastník, který vystupuje jako prostředník mezi komunikujícími stranami. [2]



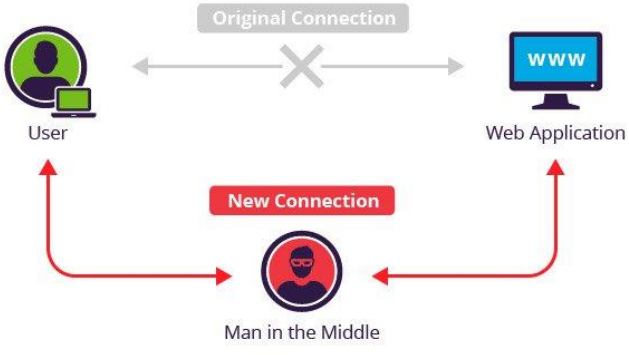
Obrázek 4 – Odposlech bezdrátové komunikace, zdroj: https://www.vpngate.net/en/images/overview_2.jpg

3.6.4 Využití rozhraní správy

Tento druh útoku se může stát problémem, když využíváte některá zařízení, které vám umožňují ovládat vaše přístupové body prostřednictvím webových rozhraní nebo přístupem z konzole. Výchozí přihlašovací údaje jsou na internetu široce dostupné, takže je nutné zajistit, aby všechna zařízení byla dostatečně zabezpečena a zabránilo se tak neoprávněnému přístupu. [3]

3.6.5 Man in the middle

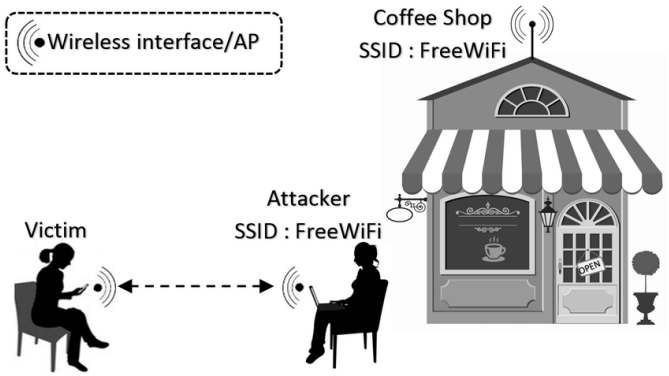
Man in the middle (MITM) je druh útoku, kdy útočník vstoupí bez jejich vědomí do komunikace mezi dvěma stranami, mění komunikaci a stává se aktivním prostředníkem. MITM se používá ke sledování šifrované komunikace, do které by se jinak nikdo nedostal. Při odposlechu bez vědomí komunikujících stran se používají falešné SSL certifikáty. Tím si strany myslí, že komunikují platným a správným certifikátem, ale přitom je certifikát útočníka, který si celou komunikaci dešifruje, a to ještě před doručením na server. Pokud útočník data znovu zašifruje, tak příjemce vůbec neví, že data jsou kompromitovaná. Princip MITM využívají i různé bezpečnostní programy, jako jsou antiviry. [22]



Obrázek 5 – Man in the middle, zdroj: https://www.imperva.com/learn/wp-content/uploads/sites/13/2019/01/man-in-the-middle-mitm.jpg

3.6.6 Bezdrátové únosy

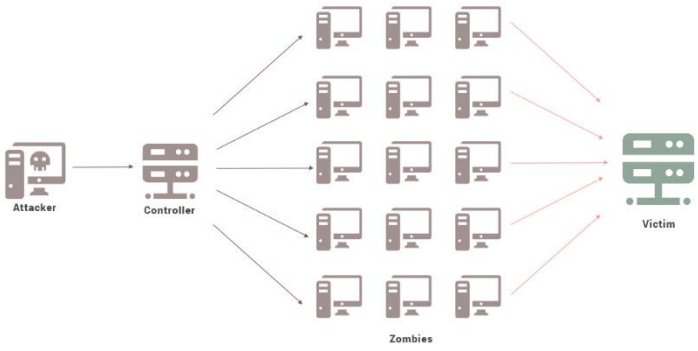
K tomu dochází v situacích, kdy útočník nakonfiguruje svoje přenosné zařízení tak, aby vysílalo jako bezdrátový přístupový bod pomocí stejného SSID jako veřejný hotspot, tzv. evil twin. Následně čeká a nic netušící oběti se k němu připojí, myslící si, že se jedná o skutečný veřejný hotspot. To je ale nechává jejich zařízení otevřené vůči útokům typu peer-to-peer a odposlechu síťové komunikace. [3]



Obrázek 6 – Evil twin, zdroj: https://www.researchgate.net/profile/Omar_Nakhila

3.6.7 DDoS

Hlavní náplň DDoS (Distributed denial of service) útoku je, aby cílové webové služby a síťová zařízení byla nedostupná a nepoužitelná pro uživatele. Dělá se to tak, že se na konkrétní síťová zařízení posílají různé zprávy, požadavky či falešné pakety až do přehlcení serverů, které přestávají zpracovávat požadavky od uživatelů. Útok po přehlcení serverů nadále pokračuje a je i dost pravděpodobné, že si útočník řekne o nějaké výkupné v kryptoměně, aby po zaplacení útok odvolal. Pro útok se používají, tzv. „zombies“, což jsou zařízení nakažena malware, která na vyžádání útočníka umí zpracovávat požadavky dle potřeby. Souhrnný název pro tuto praktiku je DDoS botnet. [6]



Obrázek 7 – DDoS, zdroj: https://static.cdn-cdpl.com/source/998b78e349061b4971c0a2b0e8d6be41/ddos-attack.png

3.6.8 Útok hrubou silou

Útok hrubou silou (Brute-Force Attack) je jednoduchý a z analytického pohledu vždy úspěšný. Při útoku se zkouší všechny kombinace hesel a uživatelského jména z dané abecedy, což je časově velmi náročné, ale ne nemožné. Pokud útočník zná název účtů a maximální délku hesla, tak zákonitě heslo prolomí. Útoku hrubou silou napomáhají nejvíce samotní uživatelé, kteří si volí velmi slabá a prolomitelná hesla. Útok hrubou silou je dále kombinovatelný s dalšími metodami útoku např. slovníkovým útokem, kde se doplňují známá slova s dalšími možnostmi. [23]

Pro zamezení prolomení hesel ve firmách se používá, tzv. politika hesel. Tato politika přesně specifikuje např. počet znaků hesla, požadované znaky, platnost hesla, po kolika neúspěšných pokusech se heslo zablokuje a na jak dlouho.

3.6.9 Sociální inženýrství

Na rozdíl od všeobecného přesvědčení není nejúspěšnějších útoků dosaženo skripty, softwarem nebo nástroji, ale sociálním inženýrstvím. Jedná se o techniku používanou k manipulaci lidí s rozdáváním informací, jako jsou počítačová hesla, nebo informací, které útočníkům pomohou omezit složitost potenciálního hesla. Nejlepší způsob, jak se vypořádat s touto potenciální hrozbou, je zajistit, aby lidé byli poučeni o bezpečnostních postupech, jako je pravidelná změna hesel a zákazu sdílení bezpečnostních tajemstvích. [24]

3.7 Útočníci

Útočník či narušitel je osoba, která již získala anebo se snaží získat neoprávněný přístup do informačních systémů za pomoci podvodného jednání. Útočníci se dají rozlišit do specifických kategorií dle jeho polohy, odbornosti a typu. [6]

3.7.1 Rozdělení dle polohy

Insider je útočník, který se připojuje do počítačové sítě zevnitř. Osoby, které provádějí útoky, mají oproti externím útočníkům zřetelnou výhodu, protože mají autorizovaný přístup do systému a také mohou znát síťovou architekturu a systémové zásady. Kromě toho může být vytvořeno menší zabezpečení proti útokům zevnitř, protože mnoho organizací se hlavně zaměřuje na ochranu před vnějšími útoky. [6]

Outsider je útočník, který nemá oprávněný přístup do konkrétní počítačové sítě. Do dané sítě se snaží získat přístup jakýmkoliv způsobem např. podvodným jednáním, vydíráním, pomocí bezpečnostních chyb či různých nedostatků, které jsou v dané síti. [6]

3.7.2 Rozdělení dle odbornosti

Amatéři mají nízkou či střední úroveň znalostí a nevlastní sofistikované vybavení pro hacking. Jejich útoky jsou méně nebezpečné, protože pro svoji nelegální činnost používají již opravené nebo zveřejněné bezpečnostní chyby, které jsou vystaveny na internetu. [6]

Profesionálové mají vysokou úroveň znalostí a vybavení, které je děláno přímo pro hacking. Tito útočníci jsou schopni provádět velice nebezpečné útoky, hlavně díky tomu, že jsou schopni vymyslet úplně nové způsoby útoku a nacházet nové bezpečnostní chyby. [6]

3.7.3 Rozdělení dle typu

White hat (etický hacker) využívá své dovednosti spíše k dobrému než zlému. White hat, také známí jako „etičtí hackeři“, mohou být někdy placenými zaměstnanci nebo dodavateli, kteří pracují pro společnosti jako bezpečnostní konzultanti, kteří se pokoušejí najít bezpečnostní díry pomocí hackerství. Používají stejné metody hackování jako black hat, až na jednu důležitou výjimku – dělají to nejprve se svolením vlastníka systému, což proces dělá zcela legálním. Testují penetrace systému, bezpečnostní systémy na místě a provádějí hodnocení zranitelnosti společností. Existují dokonce kurzy, školení, konference a certifikace pro etické hackování. [25]

Grey hat (mezityp) jsou směsí činností jak white hat, tak i black hat. Grey hat často hledají zranitelnosti v systému bez souhlasu nebo znalosti vlastníka. Pokud se vyskytnou zranitelnosti, oznámí je vlastníkovi a někdy požádají o malý poplatek za vyřešení problému. Pokud majitel neodpoví nebo nedodrží termín, hackeři někdy zveřejní nově nalezené nedostatky online tak, aby je mohl vidět svět. Tento typ hackování je však stále považován za nezákonný, protože hacker neobdržel povolení od vlastníka před pokusem o útok na systém. [25]

Black hat (cracker) má obvykle rozsáhlé znalosti o proniknutí do počítačových sítí a obcházení bezpečnostních protokolů. Jsou také zodpovědní za psaní malwaru, což je metoda používaná k získání přístupu k těmto systémům. Jejich primární motivací je obvykle osobní nebo finanční zisk, ale mohou se také podílet na kybernetické špionáži, protestech nebo možná jen být závislí na vzrušení z počítačové kriminality. Black hats se mohou pohybovat od amatérů, kteří šíří malware, až po zkušené profesionály, kteří se snaží ukrást data, zejména finanční informace, osobní informace a přihlašovací údaje. Black hats se nejen snaží data ukrást, ale také se snaží data modifikovat nebo zničit. [25]

3.8 Bezpečnost počítačové sítě

Bezpečnost počítačové sítě je proces přijímání fyzických a softwarových preventivních opatření k ochraně síťové infrastruktury před neoprávněným přístupem, zneužitím, nesprávnou funkcí, úpravou, zničením nebo nesprávným zveřejněním. Tímto procesem se tedy vytvoří bezpečná platforma pro síťové prostředky, uživatele a programy tak, aby mohly provádět povolené kritické funkce v bezpečném prostředí. Pro maximalizaci bezpečnosti sítě je potřeba používat správně navrženou a správně implementovanou bezpečnostní politiku. [2]

3.8.1 Bezpečnostní politika

Bezpečnostní politika má nastínit klíčové položky v organizaci, které je třeba chránit. To může zahrnovat síť společnosti, data, její fyzickou budovu a další. Musí také nastínit potenciální hrozby pro tyto položky. Pokud se dokument zaměří na kybernetickou bezpečnost, hrozby by mohly zahrnovat hrozby zevnitř, jako například možnost, že nespokojení zaměstnanci odcizí důležité informace, spustí interní virus v síti společnosti nebo fyzicky poškodí síťové prostředky. Alternativně by útočník z vnější strany společnosti mohl proniknout do interních systému a způsobit ztrátu dat, změnu, odcizení nebo jejich zveřejnění.

Pokaždé když jsou hrozby identifikovány, musí být stanovena pravděpodobnost, že k nim skutečně dojde. Společnost musí také určit, jak těmto hrozbám zabránit. Zavedení určitých zaměstnaneckých zásad, jakož i silné fyzické a síťové zabezpečení, by mohlo být několika zárukami. Musí existovat plán, co dělat, když se hrozba skutečně objeví. Bezpečnostní politika má být přístupná všem ve společnosti a proces bezpečnostní politiky je pravidelně přezkoumáván a aktualizován, jakmile se objeví nové hrozby. [2]

3.8.2 Bezpečnostní služby v počítačových sítích

Samotná bezpečnost zahrnuje spoustu hledisek, u kterých se důležitost mění dle specifického prostředí a požadavků konkrétního systému. Tato hlediska se dají rozdělit do následujících skupin: [2]

Autentizace

Je kladen požadavek na správnou a jednoznačnou identifikaci autora zprávy. Je tedy nutné do komunikačních protokolů vložit kvalitní autentizační mechanismus, protože jedině tak bude pro útočníka obtížné podvrhnout zfalšovanou zprávu s neznámým původem. Je velmi důležité zařadit autentizaci do komunikace, a to hlavně mezi stranami, které spolu jednoznačně nesousedí, a jediné spojení je právě síť.

V rámci autentizace existují dvě služby: Autentizace odesílatele a Autentizace spojení. Autentizace odesílatele autentizuje jen odesílatele zprávy, ale Autentizace spojení poskytuje autentizace v rámci celého navázaného spojení a zabraňuje útočníkovi duplikovat zprávy. [26]

Autorizace (řízení přístupu)

Síťová služba Řízení přístupu může stanovat pro přístup pravidla, dle nichž povoluje přístup. Přístup slouží jako ochrana před neautorizovaným použitím síťových prostředků a je závislý na identitě klienta. Často se autorizační služba dává na úroveň operačního systému nebo aplikace namísto síťových protokolů. [26]

Dostupnost

nám říká, že každá nabízená služba v počítačové síti musí být kdykoliv dostupná každému oprávněnému uživateli. Je tedy potřeba stanovit určité mechanismy, které zamezí útokům typu odepření služby. Pro nastavení těchto mechanismů slouží například stanovení limitů pro uživatele a procesy, kterým se nastaví maximální alokace prostředků. Pro zajištění odpovídající dostupnosti je také nutné zajistit bezpečnost fyzického rozložení počítačové sítě. [26]

Důvěrnost

Důvěrnost může být požadována komunikujícímu stranami. To nám značí, že komunikace nemůže být odposlouchávána žádnou jinou neoprávněnou stranou. Tato komunikace musí být tedy šifrována dobrým algoritmem s uspokojivou délkou klíče. [26]

Služby v rámci důvěrnosti:

- **Služba důvěrnost přenosu zpráv** – ochrana před neautorizovaným odhalením bez ohledu na navázaná spojení
- **Služba důvěrnost spojení** – ochranu před neautorizovaným odhalením v rámci navázaného spojení.
- **Služba důvěrnost toku dat** – zabraňuje útočníkovi znalosti toku dat
- **Služba selektivní důvěrnost** – zajišťuje důvěrnost jen některých částí přenášených zpráv

Integrita

Zachování integrity zasílaných zpráv je nejžádanější vlastnost přenosu dat v rámci počítačové sítě. Přenášená data nesmí modifikována, zdržována nebo opakovaně vysílána neautorizovanou stranou. [26]

Služby v rámci integrity:

- **Služba integrity přenosu zpráv** – ochrana před neautorizovanou modifikací bez ohledu na navázaná spojení

- **Služba integrity spojení** – ochranu před neautorizovanou modifikací v rámci navázaného spojení.
- **Služba selektivní integrity spojení** – zajišťuje integritu jen některých částí spojení
- **Služba selektivní integrity zpráv** – zajišťuje integritu jen některých částí přenášených zpráv

Nepopiratelnost

V rámci nepopiratelnosti je nutné zajistit, že žádná ze zúčastněných stran nemůže popřít svou účast na výměně dat, to ani po ukončení komunikace. Pro zaručení nepopiratelnosti v elektronické komunikaci se využívají elektronické podpisy a kvalifikované elektronické pečetě.

Nepopiratelnost zajišťují dvě služby: Nepopiratelnost odesílatele a Nepopiratelnost doručení, které slouží k tomu, aby odesílatel mohl prokázat protistraně, že daná zpráva byla odeslána při případných sporech. [26]

3.8.3 Šifrování

Šifrování je způsob úpravy čitelných dat tak, aby přenášeným informacím mohli porozumět pouze oprávněné strany. Naopak neoprávněným stranám se šifrovaná data jeví náhodná a nesmyslná. Z technického hlediska je to proces převodu prostého textu na šifrovaný text. Šifrování vyžaduje použití šifrovacího klíče: množiny matematických hodnot, které zná jak odesílatel, tak příjemce šifrované zprávy. [6]

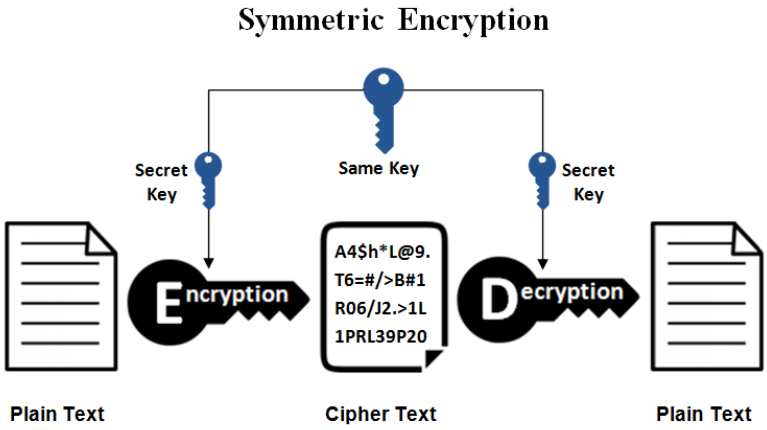
Symetrické šifrování

Symetrické šifrování je typ šifrování, při kterém se k šifrování i dešifrování elektronických informací používá pouze jeden tajný klíč. Použitím symetrických šifrovacích algoritmů jsou data převedena do formy, které nemůže pochopit kdokoli, kdo nemá tajný klíč, který ji dešifruje. Jakmile má určený příjemce, který má klíč zprávu, algoritmus obrátí svou činnost tak, aby se zpráva vrátila do své původní a srozumitelné podoby. Tajným klíčem, který odesílatel i příjemce používají, může být konkrétní heslo, kód nebo náhodný řetězec písmen nebo čísel, který byl vygenerován zabezpečeným generátorem náhodných čísel (RNG). Velmi důležité je při tomto typu šifrování důkladně zabezpečit tajný klíč a s tím spojená častá obměna daného klíče. [27]

DES (Data Encryption Standard) byl první standardizovanou šifrou pro zabezpečení elektronických komunikací a používaný ve variantách např. 2-klíčový nebo 3-klíčový (3DES). Původní DES z roku 1977 se již nepoužívá, protože je považován za prolomený, a to kvůli výkonu moderních počítačů. Ani 3DES není doporučován, stejně jako všechny

64bitové šifry. 3DES se však stále používá v čipových kartách EMV, což jsou debetní a kreditní karty. [27]

AES (Advanced Encryption Standard) je nejběžněji používaným symetrickým algoritmem, který byl původně známý jako Rijndael z roku 1997. AES je norma stanovena v roce 2001 americkým Národním institutem pro standardy a technologie pro šifrování elektronických dat. Tento standard nahrazuje DES, který byl používán od roku 1977. Šifra AES má velikost bloku 128 bitů a může mít různé délky klíčů např. AES-128, AES-192 a AES-256. [27]



Obrázek 8 – Symetrické šifrování, zdroj: https://www.ssl2buy.com/wiki/wp-content/uploads/2015/12/Symmetric-Encryption.png

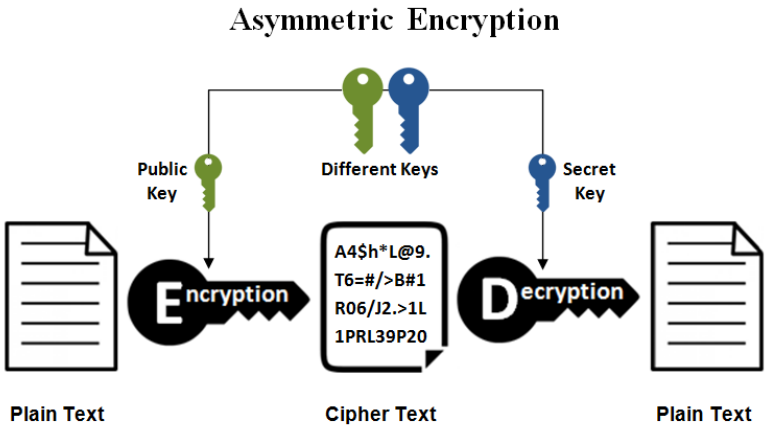
Asymetrické šifrování

Asymetrické šifrování je také známo jako kryptografie s veřejným klíčem. Pro šifrování a dešifrování dat se používá pár navzájem odkazujících se klíčů, jeden je veřejný a druhý soukromý. Veřejný klíč je volně k dispozici každému na internetu, kdo vám může chtít zaslat zprávu. Soukromý klíč je udržován na bezpečném místě a znám je jen vlastníkovi. Zpráva šifrovaná pomocí veřejného klíče může být dešifrována pouze pomocí soukromého klíče, zatímco zpráva šifrovaná pomocí soukromého klíče může být také dešifrována pomocí veřejného klíče. [28]

Asymetrické šifrování se využívá v každodenních komunikačních kanálech, zejména přes internet. Populární algoritmus šifrování asymetrického klíče zahrnuje EIGamal, RSA, DSA, techniky eliptické křivky a PKCS. [28]

RSA (Rivest–Shamir–Adleman) je šifrovací technologie veřejného klíče vyvinutá společností RSA Data Security. Algoritmus RSA je založen na složitosti faktorizace velmi velkých čísel. Prolomení klíče RSA tedy vyžaduje obrovské množství času a výpočetního

výkonu. Je to standardní metoda šifrování důležitých dat, zejména dat přenášených přes internet. [6]



Obrázek 9 – Asymetrické šifrování, zdroj: https://www.ssl2buy.com/wiki/wp-content/uploads/2015/12/Asymmetric-Encryption.png

3.9 Bezpečnostní opatření Wi-Fi sítě

Jedná se o prevenci sloužící k tomu tak, aby se to vnitřní sítě nějakého konkrétního subjektu nedostali neoprávnění uživatelé, kteří by chtěli v síti páchat určitou škodu. Pro danou prevenci se vytvořily a jistě i vytvoří nové postupy a standardy, protože se každým dnem zlepšuje umění hackingu ve světě.

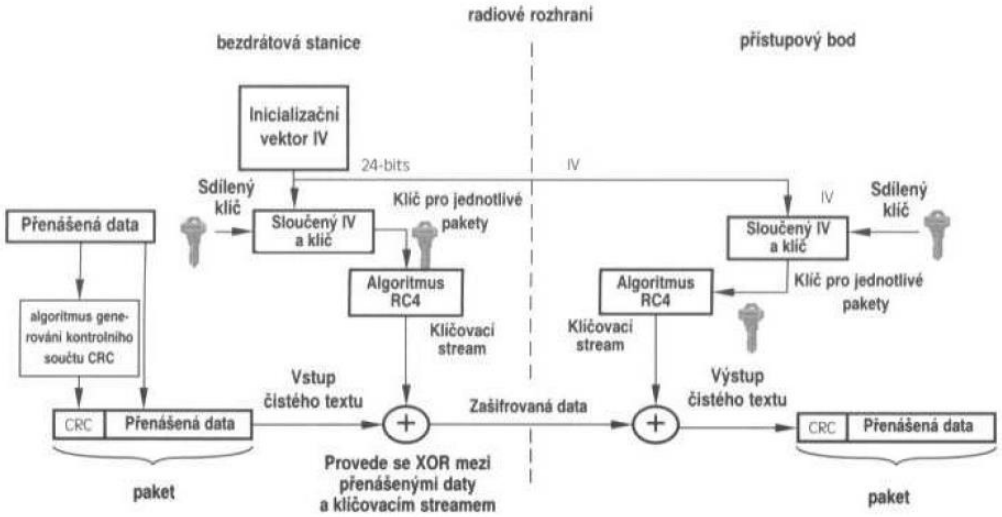
3.9.1 WEP

WEP (Wired Equivalent Privacy) je to zastaralý protokol pro zabezpečení v bezdrátových sítích. Byl vytvořen jako součást původního standardu IEEE 802.11 v roce 1997. Byl používán pro zařízení se standardy IEEE 802.11a a IEEE 802.11b předtím, než byl vytvořen standard WPA. Tento protokol byl vytvořen za účelem poskytnutí podobného zabezpečení jako drátové připojení např. kroucená dvojlinka. protože bezdrátový přenos sebou nese rizika odposlechu na větší vzdálenost bez potřeby fyzického kontaktu s danou sítí. [5]

Protokol WEP používal symetricky streamovanou šifru **RC4**, tedy šifru s tajným klíčem. Tato šifra pracuje tak, že se po odesílaná zpráva šifruje dle nějakého klíče (slova nebo sekvence znaků) a na cílovém bodě se zase podle tohoto klíče dešifruje. Klíč se během přenosu expanduje v pseudonáhodném klíčovém streamu, který má stejnou délku jako má šifrovaná zpráva. O vygenerování expanze se stará **PRNG** (generátor pseudonáhodných čísel). Jsou to pravidla, dle nichž se klíč rozšíří na délku zprávy do klíčovacího streamu. Šifrování a rozšifrování dat je velmi jednoduché, díky logické operace **XOR** s klíčovým

streamem. Zařízení, která mají toto šifrování provozovat, tak musí mít stejně nastavené PRNG a musí znát tajný klíč (v podstatě se tedy nejedná o tajný klíč). Tajný klíč měl definovanou velikost 40 bitů a používal v předsadí 24bitový inicializační vektor IV, který se používal pro pseudonáhodný klíčový stream. Velikost tajného klíče byla malá, a proto někteří výrobci začali používat vlastní délku šifry buď 128 bitů nebo 256 bitů, ale tyto experimenty nebyly podporovány protokolem WEP, a mohlo to zapříčinit nemožnost zařízení komunikovat. Pro zajištění integrity dat WEP používal metodu kontrolního součtu **CRC-32**. [5]

V srpnu roku 2001 došlo k prolomení protokolu WEP, a proto byl plošně nahrazován zabezpečením WPA2 dle standardu IEEE 802.11i. [5]



Obrázek 10 – WEP, zdroj: [5]

3.9.2 WEP2

Nová verze původního WEP byla již přítomna v některých z prvních návrhů standardu **IEEE 802.11i**. Za úkol měla vylepšit zabezpečení, kde se snaží odstranit známé nedostatky původního WEP. Pro lepší zabezpečení WEP2 rozšiřoval inicializační vektory a zesiloval šifrování na 128bitové klíče. WPA2 měl po svém uvedení nakonec stejné bezpečnostní problémy jako původní WEP, ale s tím rozdílem, že útočníkovi to zabere o něco více času. Od plošného nasazení WEP2 se ustoupilo, protože byl prohlášen jako deficitní, a potřeboval by spousty oprav. Některé funkce WEP2 se použili až pro WAP např. prodloužené délky klíčů (TKIP WPA). [4]

3.9.3 WPA

WPA (Wi-Fi Protected Access) plně nahrazuje WEP po jeho prolomení v roce 2001. Zabezpečení WPA bylo ratifikováno sdružením Wi-Fi Alliance v roce 2002 jako dočasné řešení před příchodem standardu IEEE 802.11i.

WPA již při svém uvedení byl dopředu kompatibilní se standardem 802.11i. Pro šifrování komunikace se nově využívá **TKIP** (Temporal Key Integridy Protocol) s šifrou RC4 jako u WEP, a proto je i zpětně kompatibilní. V rámci zabezpečení se využívá standardně 128bitový klíč a naproti WEP obsahuje dynamické dočasné klíče (TKIP), jenž se mění každých 10 000 paketů. Další výhoda TKIP je **MIC** (Message Inegrity Check), tedy kontrola integrity zpráv. Je mnohonásobně bezpečnější než původní kontrolní součet CRC. Má za úkol znemožnit útočníkovi změnu zprávy během přenosu, ale i po přenosu. Je to docíleno tím, že jednotlivé rámce obdrží digitální podpis, který zamezí útokům typu **Man in the middle**. TKIP dále čísluje jednotlivé pakety a tím eliminuje útoky typu **replay** (útok přehráním). Celkově se již původní WPA nedoporučuje používat, protože byl již nahrazen bezpečnějšími variantami, které jsou WPA2 a WPA3. [5]

3.9.4 WPA2 (standard IEEE 802.11i)

V červnu roku 2004 konečně vyšel standard IEEE 802.11i, který byl normován sdružením **Wi-Fi Alliance** a dostal označení WPA2. Je i zpětně kompatibilní s původním WPA. Od dne 13. března 2006 vznikla povinnost certifikace WPA2 pro všechna nová zařízení, která chtějí být certifikována jako Wi-Fi zařízení. WPA2 přinesl novinku, kterou byl šifrovací protokol **CCMP** (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol), který nahradil TKIP. Protokol pracuje na režimu čítače **CCM** a šifrovacího standardu **AES**, jenž má velikost klíče 128bitů, a daný klíč se neustále mění. [29]

Standard IEEE 802.11i pro Wi-Fi sítě je označen jako **RSN** (Robust Security Network). Protokol RSN nám slouží pro autentizaci, silnou distribuci klíčů a nové mechanismy k zajištění integrity. Zařízení s protokolem RSN je ve velkém množství schopné komunikovat se zařízeními, která podporují protokol RSN. Architektura standardu IEEE 802.11i je definována jako **TSN** (Transitional Security Network), ve kterém se právě nachází protokol RSN. Použití čtyřfázového handshake pro autentizaci a asociace se nazývá **RSNA** (Robust Security Network Association). [30]

V roce 2016 došlo k prolomení WPA2 pomocí **KRACK** (Key Reinstallation Attack), které se týkalo všech zařízeních a všech operačních systémů, které používají WPA.

Dané prolomení způsobovalo neoprávněné odcizení všech dat konkrétního zařízení. Chyba byla naštěstí včas odhalena a nahlášena, a proto výrobci byli schopni své výrobky včas zafixovat. [31]

3.9.5 WPA3

V lednu roku 2018 byl oznámen nový standard WPA3, který bude plně nahrazovat standard WPA2. WPA3 si zachovává kompatibilitu se zařízeními WPA2 a je zatím jen volitelnou certifikací pro zařízení Wi-Fi CERTIFIED. Postupem času bude nastaven jako standard s tím, jak bude růst jeho podíl na trhu. [32]

Wi-Fi sítě se liší v účelu použití a potřebách zabezpečení. WPA3 obsahuje další funkce speciálně pro osobní a podnikové sítě. Uživatelé **WPA3-Personal** dostávají zvýšenou ochranu před pokusy o odhad hesla, a to i u hesel, která nesplňují typické doporučení týkající se složitosti. Tato schopnost je povolena pomocí **SAE** (Simultaneous Authentication of Equals), která nahrazuje **PSK** (předsdílený klíč) ve WPA2-Personal. Tato technologie je odolná proti útokům offline slovníku, kdy se protivník pokusí určit síťové heslo vyzkoušením možných hesel bez další interakce se sítí. [32]

Hlavní rysy WPA3-Personal jsou:

- **Přirozený výběr hesla:** Umožňuje uživatelům zvolit si hesla, která se snáze zapamatují.
- **Snadné použití:** Poskytuje vylepšené ochrany beze změny způsobu, jakým se uživatelé připojují k síti.
- **Přední tajemství:** Chrání datový provoz, i když je po přenosu dat heslo prolomeno.

Uživatelé **WPA3-Enterprise** nyní mohou využívat citlivé datové sítě pro vyšší stupeň zabezpečení. WPA3-Enterprise staví na WPA2 a zajišťuje jednotné používání bezpečnostních protokolů v síti. [32]

Hlavní rysy WPA3-Enterprise jsou:

- **Ověřené šifrování:** 256bitový Galois Counter Mode Protocol (GCMP-256).
- **Odvození a potvrzení klíče:** 384bitový Hashed Message Authentication Code (HMAC) s algoritmem Secure Hash Algorithm (HMAC-SHA384).
- **Stanovení klíče a ověření:** Výměna eliptické křivky Diffie-Hellman (ECDH) a algoritmus digitálního podpisu eliptické křivky (ECDSA) pomocí 384bitové eliptické křivky.
- **Robustní ochrana rámce správy**: 256bitový protokol pro ověřování integrity protokolu Galois Message (BIP-GMAC-256).

Dále nabízí volitelný režim využívající 192bitové bezpečnostní protokoly o minimální síle a kryptografické nástroje pro lepší ochranu citlivých dat. 192bitový režim

zabezpečení nabízený WPA3-Enterprise zajišťuje správnou kombinaci kryptografických nástrojů a nastavuje konzistentní základní úroveň zabezpečení v síti WPA3. [32]

3.9.6 Ukrytí SSID

Nám značí, že identifikátor bezdrátové sítě (**SSID**) je pro ostatní zařízení ukrytý. Přístupový bod (**AP**) obsahuje nastavení ohledně viditelnosti SSID. Administrátor zde může zvolit viditelnost či neviditelnost daného identifikátoru. Nastavení se používá pro zajištění větší bezpečnosti dané sítě, protože uživatel, který se chce k Wi-Fi připojit, tak musí znát jak název, tak i heslo. Celkově tato metoda bezpečná není, protože se SSID posílá v plain text formátu (v prostém textu) a je tedy možné ho odposlechnout. Proto se pro přihlášení k Wi-Fi může požadovat např. i certifikát, který nejlépe vydala vnitřní certifikační autorita tak, aby byla zajištěna bezpečnost sítě.

3.9.7 Filtrování MAC adres

Je funkce přístupového bodu, která umožnuje administrátorovi specifikovat seznam povolených a zakázaných MAC adres, které se mohou k bodu připojit. Administrátor pro specifikaci MAC adres používá whitelist pro povolení a blacklist pro zakázání. Tuto metodu lze obejít tím, že útočník v probíhající síťové komunikaci odposlechne MAC adresu na úrovni paketů a poté si ji na svém zařízení nastaví. Po nastavení povolení MAC adresy dostává útočník možnost přihlásit se do dané sítě a tím síť infiltruje.

3.9.8 ACL

Seznam řízení přístupu (**ACL** – Access Control List) je seznam pravidel, která řídí síťový provoz a zvyšují bezpečnost sítě na základě kritérií pro filtrování na přístupovém bodu. Pomocí ACL můžeme definovat jaké odchozí/příchozí porty, protokoly nebo síťové aplikace budou dostupné konkrétním klientům v síti či v síti obecně. [33]

Výhody ACL:

- Omezení síťového provozu
- Zvýšení výkonu sítě
- Zajištění řízení toku dat v síti
- Omezení přístupu v síti
- Podrobná kontrola vstupu a výstupu ze sítě

3.9.9 VPN

Virtuální privátní síť (**VPN** – Virtual Private Network) je šifrované a zabezpečené propojení mezi dvěma sítěmi nebo mezi uživatelem a sítí do jedné soukromé sítě. Inicializace propojení může být vyvolána kdekoliv v sítí internet, je-li to v danou chvíli

možné. Propojením se vytvoří šifrovaný tunel, kterým je vedena veškerá komunikace mezi zařízením a privátní sítí za pomoci šifrovacího protokolu. Zařízení připojené do VPN získá falešnou IP adresu, která vystupuje jako IP adresa zařízení správce VPN. Funkci VPN využívají hlavně firmy z důvodu bezpečnosti a možnosti se připojit kdekoliv do vnitřní sítě organizace. VPN se využívá i v domácnostech, jako kombinace se sítí typu P2P (Peer-to-Peer) pro přenos dat anebo možnosti obejít cenzuru internetových stránek daným státem. [34]

Příklady šifrovacích protokolů VPN:

PPTP (Point-to-Point Tunneling Protocol) byl nejslabší protokol v rámci VPN připojení, protože používal jen 128bitovou šifru. Vytvořen byl v roce 1990 a od jeho prolomení v roce 2012 ho nelze považovat již za bezpečný. [35]

IPsec (IP Security) je protokol, který vznikl jako povinná součást implementace IPv6 v druhé polovině 90. let 20. století a je standardizován sdružením **IETF** (Internet Engineering Task Force). Tento šifrovací protokol má dva provozní režimy, kterými jsou režim přenosu (transportní) a režim tunelu. Hlavní rozdíl je, že v režimu přenosu se šifruje a ověřuje pouze obsah daného paketu a v režimu tunelu se šifruje a ověřuje celý paket. [36]

OpenVPN je volně dostupný software včetně zdrojového kódu pro možnost vytvoření vlastního šifrovaného VPN tunelu. Software byl vytvořen Jamesem Yonanem a publikován pod licencí **GNU GPL** (GNU General Public License). Největší výhoda tohoto řešení je široká podpora operačních systémů a podpora komunitního řešení. [37]

3.9.10 Firewall

Firewall je zařízení či software oddělující síťový provoz mezi dvěma počítačovými sítěmi s různou úrovní důvěryhodnosti a zabezpečení (např. vnitřní sít a sít internet). Data jsou propouštěna dovnitř či ven ze sítě na základě předdefinovaných nebo dynamicky utvářených pravidel a politik. Hlavní účel firewallu je ochrana dat před neoprávněným únikem bez souhlasu vlastníka a neoprávněným průnikem útočníka do sítě. U domácností a firem je brána firewall nejzákladnějším, nejefektivnějším a nejdůležitějším prvkem pro ochranu dané sítě. Je důležité bránu firewall kombinovat ještě s antivirovým a antispywarovým programem na zařízeních v dané síti, a to ještě před připojením k sítí internet. Tyto programy slouží jako sekundární ochrana sítě, a tedy není dobré na nich šetřit. [38]

Firewally lze rozdělit do tři základních skupin:

Paketové filtry: jedná se o nejjednodušší a také nejstarší formu firewallů, které jsou často implementovány na routerech. Vyznačují se vysokou rychlostí zpracování požadavků, ale nízkou úrovní zabezpečení pro procházející spojení u složitějších protokolů jako jsou např. FTP nebo video/audio streaming. Funkce paketového firewallu spočívá v kontrole zdrojové adresy, cílové adresy a portu dle nastavených pravidel. Kontrola probíhá na síťové a transportní vrstvě modelu OSI. Paketové firewally neumožňují logování událostí a nejsou ani schopné upozornit administrátora na podezřelé aktivity. Typickým představitelem paketových filtrů je ACL (Access Control Lists), který byl vysvětlen v kapitole ACL. [38]

Aplikační brány (Proxy firewall): jsou bezpečnější než jednoduché paketové filtry, protože zcela oddělují chráněnou a nedůvěryhodnou síť, mezi které jsou postaveny. Jsou ale pomalejší při zpracovávání požadavků, protože se kontrolují všechny pakety dané služby, náročné na HW a omezují uživatele na okruh služeb, které jsou na proxy povoleny. Je nutné u proxy mít povolený jen omezený počet služeb tak, aby byla zajištěna bezpečnost. Veškerá komunikace přes proxy probíhá dle spojení klient a server. Klient se připojí na proxy, která spojení zpracuje a dle požadavku klienta otevře nové spojení k serveru, kde je poté klientem samotná proxy. Data, která proxy získá od serveru poté předá klientovi, který data vyžadoval. Proxy pracují na aplikační vrstvě ISO modelu, a tedy nijak nechrání samotné zařízení, na kterém proxy běží. [38]

Stavové paketové filtry: provádějí kontrolu stejně jako jednoduché paketové filtry, ale navíc si ukládají informace o povolených spojení, které používají při rozhodování. Pokud se tedy jedná o povolené spojení, tak spojení bude povoleno hned, a které povoleno není, tak bude procházet rozhodovacím procesem. Daná věc má za následek urychlení zpracování paketů u povolených spojení. Naproti aplikačním bránám je výhodou snadnější konfigurace, ale nižší bezpečnost. [38]

4 Vlastní řešení

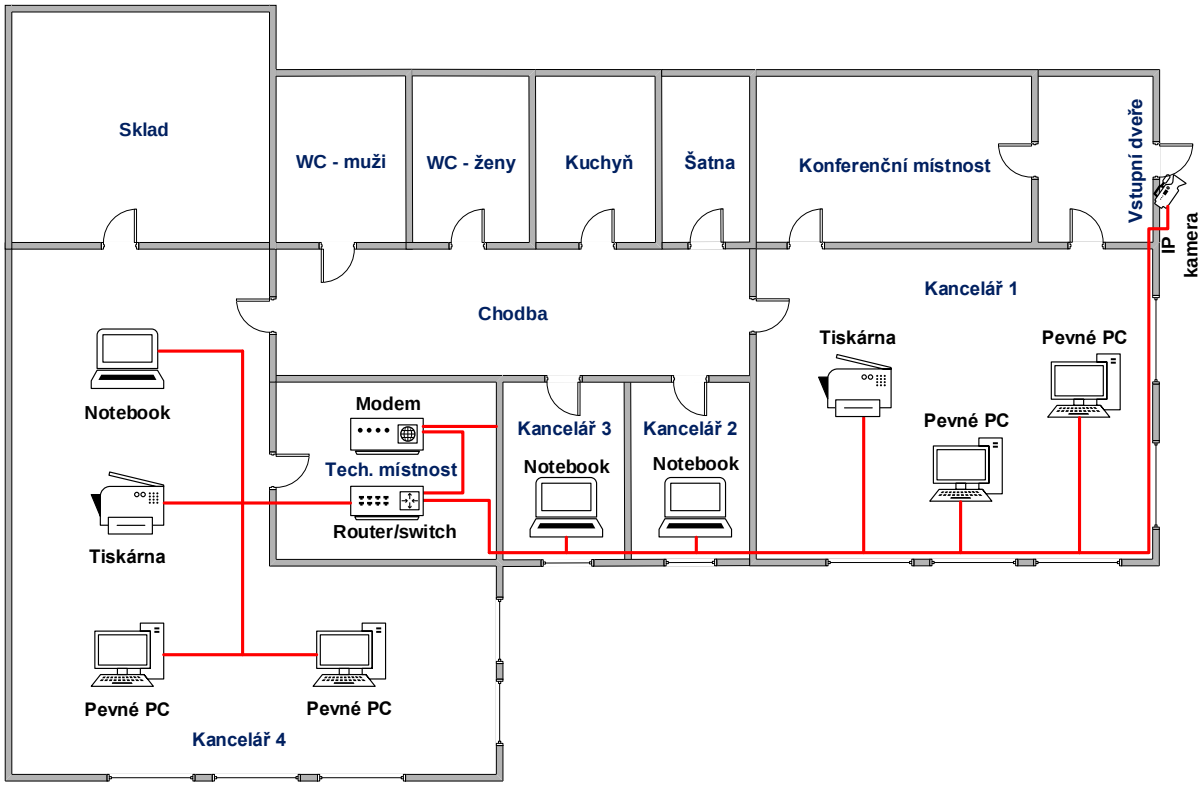
Tato kapitola se zabývá praktickou částí bakalářské práce a jejím cílem je analýza dostupných metod pro bezpečnost dat v počítačových sítích. Následuje vypracování optimálního nastavení bezpečnosti dat v síťové infrastruktuře fiktivního podniku s využitím poznatků zpracovaných v teoretické části bakalářské práce. Fiktivní podnik se zabývá vymáháním pohledávek a je sestrojen na základě reálného podniku. Praktická část má popisovat zabezpečení a nastavení bezdrátové sítě reálného podniku, ale kvůli zaměření firmy a dle § 504 zákona č. 89/2012 Sb. není možné tyto informace veřejně poskytnout.

Pro analýzu VPN řešení a analýzu metod zabezpečení pro aktuální stav podniku byla v obou případech použita metoda pořadí s váhami. Metoda pořadí je založena na uspořádaní matice kritérií dle preferencí, a poté převedení na matici pořadí. Dle stanovených kritérií se přiděluje pořadové číslo, kde nejnižší pořadí znamená nejlepší. Stanovené váhy jsou subjektivní pohled podniku a vyznačují kritérium důležitosti v rozhodovacím procesu. Pro stanovení výsledku metody pořadí s váhami se musí vypočítat skalární součin každého řádku, kde hodnota s nejnižším číslem ve výsledku je pro nás kompromisní varianta.

4.1 Popis podniku

Podnik je již delší dobu na pracovním trhu, ale v tuto chvíli neočekává nezvyklý velký příliv zakázek k vymáhání vlivem silné ekonomické situace v České republice. Vlivem této skutečnosti si podnik stanovil kritérium cena, která má být nižší s tím, že podnik bude splňovat zavedené bezpečnostní standardy v počítačových sítích. Sídlo podniku je v rezidenčním domě, kde podnik vlastní dva byty. Tyto byty jsou do sebe spojeny a celkově je to tedy 27% plochy z rezidenčního domu v jeho vlastnictví.

Pro svoji činnost podnik využívá čtyři pevné počítače, tři notebooky s dokovací stanicí, dvě multifunkční laserové tiskárny a jednu IP kameru. K pevným počítačům a dokovacím stanicím jsou připojeny běžná vybavení jako je monitor, myš, klávesnice a sluchátka. Multifunkční tiskárny i IP kamera jsou sdíleny v rámci lokální sítě.



Obrázek 11 – Plán podniku a kabeláže, zdroj: vlastní zpracování

4.2 Možné metody zabezpečení sítě

Tato část bakalářské práce specifikuje možné metody zabezpečení sítě podniku. Některé vybrané metody zabezpečení se nedoporučují ze své podstaty používat u větších firem, např. z důvodu velké časové náročnosti či zbytečné složitosti při jejich správě, ale u malého podniku je jejich využití vhodné. U jakéhokoliv metody zabezpečení je potřeba si uvědomovat, že je vždy jen na nějakou určitou dobu, než bude vzhledem ke všem okolnostem nedostatečná.

4.2.1 Zabezpečení pomocí filtrace MAC adres

Jedná se o základní zabezpečení sítě pomocí nastavení konkrétních MAC adres zařízení do filtru MAC adres. Tento filtr je obsažen v administrátorském rozhraní routeru. Po povolení daných MAC adres umožňuje zařízením se připojit k dané síti a využívat povolených služeb v síti. Pokud se bude přihlašovat zařízení, které není povoleno ve filtru MAC adres, tak bude danému zařízení odepřen přístup do sítě.

Tento typ zabezpečení má velké zastoupení u menších podniků, díky velmi snadnému přehledu o zařízeních vyskytujících se v síti. Při budoucím růstu firmy toto zabezpečení nebude optimální na správu, protože se neustále bude zvyšovat a měnit počet

zařízení, která se do sítě připojují. Každá úprava se musí ručně zapracovat do tabulky filtru MAC adres v administrátorském rozhraní routeru.

Zabezpečení má velkou slabinu v tom, že jde velmi jednoduše zjistit MAC adresa v probíhající komunikaci na úrovni paketů. Útočník tedy může odposlechnout na filtru povolenou MAC adresu. Tu si poté nastaví na své zařízení. Následně bez problému projde skrze filtr MAC adres a infiltruje síť.

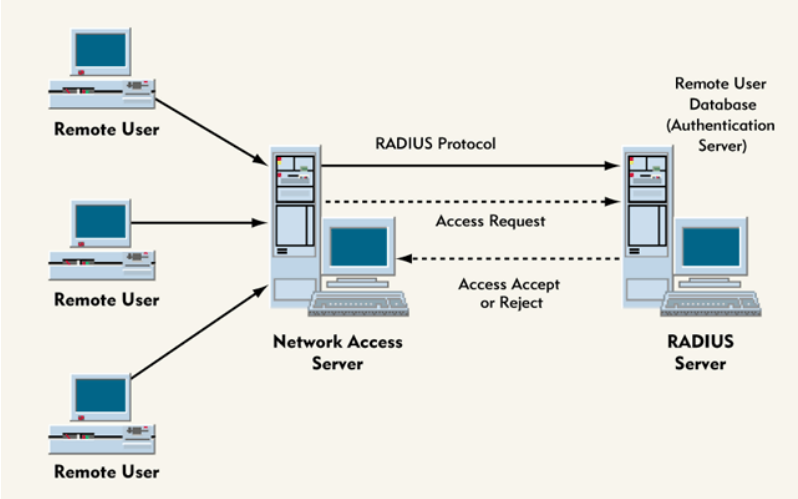
4.2.2 Zabezpečení pomocí protokolu RADIUS

RADIUS (Remote Authentication Dial in User Service) je bezpečnostní protokol, který spadá do kategorie tzv. **AAA protokolů** (Authentication, Authorization and Accounting) a je popsán ve standardu IEEE 802.1X. Protokol pro svou funkčnost využívá porty UDP/1812 a UDP/1813, které jsou pro tento protokol standardizovány. Protokol funguje v modelu Klient – Server, kde klienti fungují jako NAS (Network Access Server). NAS může být jakékoliv zařízení v síti, které má možnost sdílení dat s podporou síťových protokolů. Zařízení, která fungují jako NAS tedy odesílají data o uživatelích a připojení na RADIUS server, který je k nim přiřazen. RADIUS server po získání požadavku Acess-Request od klientů má tři úkoly: [39]

Autentizuje: ověřuje uživatelské jméno, heslo a číslo portu klientů, kteří se chtějí do vnitřní sítě připojit. Ověřuje i klienta, od kterého přišel daný požadavek, pokud ho server nezná, tak ho zahodí a neumožní mu přístup a odešle chybovou hlášku Access-Reject. Pokud klienta zná, poté server začne prohledávat databázi známých klientů, a pokud byť jeden údaj nesedí (IP, MAC, další údaje), tak klienta odmítne a neumožní mu přístup. Při úspěšném ověření všech možných údajů a povolení vstupu server zašle klientovi hlášku Access-Accept. Pro ověření využívá protokolu EAP (Extensible Authentication Protocol) zabalený do ethernetových rámců EAPOL (EAP Over LAN). EAP je dále rozšiřitelný pomocí různých druhů autentizačních metod např. EAP-TLS, EAP-TTLS, EAP-OTP, EAP-IKEv2 atd. [40]

Autorizuje: server ověřuje jaké operace mohou klienti v síti provádět.

Účtuje: sleduje využití síťových služeb klienty pro potřeby dalších možných operací jako jsou použití pro správu serveru, fakturace služeb poskytovatelem, plánování zdrojů nebo pro něco dalšího.



Obrázek 12 – Princip RADIUS serveru, zdroj: https://upload.wikimedia.org/wikipedia/commons/0/03/RADIUS-Server.gif

4.2.3 Zabezpečení pomocí Proxy serveru

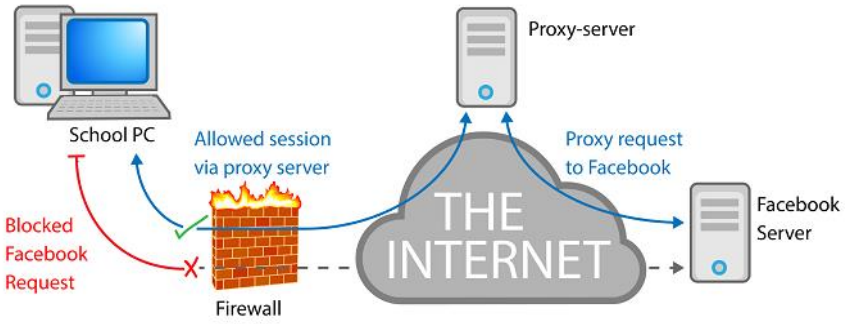
Proxy server zcela odděluje chráněnou vnitřní síť a nechráněnou vnější síť, mezi které je umístěn. Funguje tedy jako prostředník komunikace mezi klienty v lokální síti a vzdálenými zařízeními mimo tuto lokální síť. Proxy server zpracovává klientské požadavky a vůči cílovým zařízením vystupuje sám jako klient. Přijaté odpovědi zpětně odesílá na klienta, který komunikaci inicializoval. Existují různé typy proxy serverů, které mají specifické účely pro příklad si některé představíme:

Gateway (tunneling) proxy: tento typ předává nemodifikované a nefiltrované požadavky a odpovědi zařízením v síti.

Forward proxy: spolupracuje s bránou firewall a díky tomu kontroluje procházející obsah zásadami zabezpečení pro zabezpečení vnitřní sítě. Klientům v jinak omezené síti umožňuje přístup na internet jako jediný bod přístupu. Pro klienty v probíhajících komunikacích skrývá jejich IP adresu tím, že forward proxy server vystupuje do sítě internet jako klient. [41]

Reverzní proxy: se instalují v blízkosti webových serverů, protože mohou fungovat jako **load balancer** (vyvažovač zátěže). Dále snižují zátěž webových serverů pomocí načtení statického obsahu do cache a komprimace obsahu. Též spolupracuje s bránou firewall jako jediný bod přístupu a jako kontrola přenášeného obsahu pomocí zásad zabezpečení. [41]

Cachovací proxy: jedná se o nejzákladnější a nejstarší typ proxy serverů. Umožňují urychlení zpracování požadavků, snížení nákladů a zvýšení výkonu serverů, ke kterým je připojena. Je to zapříčiněno tím, že cache proxy server má u sebe uložené odpovědi z minulosti na často kladené dotazy.



Obrázek 13 – Princip Proxy serveru, zdroj: https://www.ashokcharan.com/Marketing-Analytics/images/wa03.png

4.2.4 Zabezpečení pomocí VPN

VPN řešení nabízí anonymitu a zaručenou bezpečnost přenosu pomocí šifrované komunikace. Anonymita je dosažena tím, že se klient připojuje přes VPN server, přes který dále komunikuje do sítě. Ostatním účastníkům síťového provozu se poté jeví jako onen VPN server. Bezpečnost přenosu je dosažena pomocí šifrovaného tunelu, který je mezi klientem a VPN serverem. Skrze daný tunel je vedena veškerá komunikace.

Na trhu práce roste počet profesí s možností práce z domova (home office). S tím je tedy nutné přepokládat, že tento vývoj přijde i do našeho podniku. Pro funkci VPN si podnik bude muset zvolit poskytovatele VPN či udělat vlastní řešení. Vlastní řešení je pro malý podnik zbytečně nákladné a vyplatí se až ve velké firmě. Je to hlavně díky nákladu na IT specialistu, který by dané řešení měl v gesci. Na trhu práce se průměrná cena IT specialisty pohybuje okolo 45.000,- Kč hrubého za měsíc (údaj ze začátku roku 2020).

Obrázek 14 – Princip VPN, zdroj: https://blog.avast.com/hs-fs/hubfs/how-a-vpn-works.png

4.3 Výběr VPN řešení pro možnost analýzy

Pro možnost analýzy je vybráno pět náhodných poskytovatelů VPN řešení. Podmínky pro výběr jsou, že daný poskytovatel má nějaké infrastrukturní zastoupení v České republice a nabízí své řešení aspoň na celý jeden rok. Analýza je prováděna na základě informací uvedených na webových stránkách každého poskytovatele.

Příklad VPN řešení na 1 rok:

NordVPN: Pro připojení na VPN je nutné vlastnit aplikaci NordVPN pro daný operační systém. Podporované operační systémy jsou: Android, Mac OS, iOS, Linux, Windows a další. Dále je možné využít doplněk do Google Chrome, Mozzila Firefox. V aplikaci lze vybírat pro připojení až z 5479 serverů (z toho 57 v ČR) z 57 zemí světa. Uživatelská podpora je poskytována pro 24/7 skrze FAQ (Help Center), email a online chat. Podporované protokoly jsou OpenVPN a IPSec/IKEv2 s šifrováním AES-256 a 4096bitovým RSA klíčem. Legislativní zázemí společnosti je v Panamě, která je považována za přátelskou zemi, co se týče soukromí vzhledem k chybějícím dohodám o sdílení sledování s ostatními zeměmi světa. Firma NordVPN garantuje, že nijak neloguje probíhající komunikace tzv. no-log policy. Obsahuje VPN kill-switch, který slouží jako ochrana uživatele před náhodným pádem VPN tak, aby se uživatel nemohl hned přihlásit na nezabezpečený internet, a tím byl v síti internet vidět. [42]

Služba je nabízena na rok za cenu 74.65 € až pro 6 zařízení připojených najednou. Nejlevnější plán, který je nabízen je na 3 roky a stojí 111.82 €. Dále je nabízena garance vrácení peněz, až do 30 dnů od nákupu. [42]

CyberGhost: K připojení k službě je nutné mít nainstalovanou aplikaci CyberGhost VPN, která je dostupná pro Android, Mac OS, iOS, Linux, Windows a televize s Amazon fireTV a Android TV. CyberGhost nabízí připojení k 6206 serverům (44 ČR) z 90 zemí světa. Uživatelská podpora je 24/7 skrze FAQ a online chat. Šifrování je stejné jako u NordVPN. Podpora VPN protokolů: OpenVPN, IKEv2 a L2TP/IPSec. Legislativní zázemí společnosti je v Rumunsku (Bukurešti). Jakožto člen Evropské unie, tak musí daná země splňovat vysoké nároky na právní stát a musí splňovat podmínky pro sdílení dat na světové úrovni. Jedná se tedy o neutrální umístění, které má své výhody i nevýhody. Splňuje též no-log policy a VPN kill-switch. [43]

Služba je nabízena na rok za cenu 63.48 € až pro 7 zařízení připojených najednou. Nejlevnější plán, který je nabízen je na 3 roky a stojí 88 € a jako bonus klient dostane další 2 měsíce zdarma. Za příplatek 5 € měsíčně klient může dokoupit dedikovanou IP adresu pro svá zařízení. CyberGhost nabízí garanci vrácení peněz, až do 45 dnů od uskutečnění nákupu. [43]

SurfShark: Vlastní aplikace SurfShark VPN, která slouží k připojení k VPN a má obrovskou podporu operačních systémů a zařízení. Podpora je obrovská díky kombinaci, jakou má NordVPN a CyberGhost, a navíc podporuje Apple TV a herní konzole. Bohužel

není takový výběr serverů jako u konkurence, celkově 1040 serverů ze 61 zemí světa včetně ČR (počet neznámý). Podpora je nabízena 24/7 skrze FAQ, email a online chat. Šifrování klasické AES-256 s protokoly IKEv2, OpenVPN a Shadowsocks. Legislativní zázemí jsou Britské Panenské ostrovy jakožto zámořské území Velké Británie, což je zatím člen Evropské unie (viz. CyberGhost) do doby úplného Brexitu. No-log policy a VPN kill-switch jako konkurence. [44]

Služba je nabízena na rok za cenu 59.88 € pro neomezený počet zařízení připojených najednou. Nejlevnější plán, který je nabízen je na 2 roky a stojí 69.36 €. Je nabízena garance vrácení peněz až do 30 dnů od uskutečnění nákupu. [44]

ExpressVPN: K připojení k VPN se používá aplikace ExpressVPN, která má obrovskou podporu jako SurfShark. Počet serverů pro přihlášení je něco málo přes 3000 z 94 zemí světa včetně ČR (počet neznámý). Podpora též 24/7 skrze FAQ, email a online chat. Šifrování je stejné jako konkurence s podporou protokolů: OpenVPN, L2TP/IPSec, IKEv2/IPSec a PPTP. Legislativní zázemí jako u SurfShark Britské Panenské ostrovy. Obsahuje no-log policy a VPN kill-switch. [45]

Služba je nabízena na rok za cenu 99.95 $ (91 €) až pro 5 zařízení připojených najednou s neomezenou přenosovou rychlostí. Levnější varianta není. Je nabízena garance vrácení peněz až do 30 dnů od uskutečnění nákupu. [45]

PrivateVPN: Pro funkci VPN se používá aplikace PrivateVPN, která má velmi malou podporu, a to jen Windows, MacOS, iOS a Android. Počet serverů je jen 150 v 60 zemí světa. V České republice je jediný server, kterým je: cz-pra.pvdata.host. Podpora standardně 24/7 skrze FAQ, email a online chat. Šifrování jako konkurence s podporou protokolů: OpenVPN, L2TP/IPsec, PPTP, IKEv2. Legislativní zázemí je Švédsko komentář k tomu viz. CyberGhost. Obsahuje no-log policy a nikoliv VPN kill-switch. [46]

Služba je nabízena na rok za cenu 43.20 $ (39.25 €) až pro 6 zařízení připojených najednou. Levnější varianta není. Je nabízena garance vrácení peněz až do 30 dnů od uskutečnění nákupu. [46]

4.3.1 Analýza VPN řešení

Pomocí metody pořadí s váhami byla vypočtena tabulka, která analyzuje navržené VPN řešení, která jsou vyspecifikována v kapitole 4.3. Výběr VPN řešení pro možnost analýzy. Pro možnost analýzy byla zvolena kritéria, které je možno získat od poskytovatelů a mají pro podnik význam při rozhodování.

Stanovená kritéria jsou: Podpora OS a zařízení, Počet serverů a zemí se servery, Podpora VPN protokolů, Počet připojených zařízení a Cena za 1 rok v €. Váhy kritérií byly stanoveny dle důležitosti pro podnik při rozhodovacím procesu.

Analýza VPN řešení						
Poskytovatel	**Podpora OS a zařízení**	**Počet serverů a zemí se servery**	**Podpora VPN protokolů**	**Počet připojených zařízení**	**Cena za 1 rok v €**	**Součet**
NordVPN	3,5	3	5	3,5	4	3,73
CyberGhost	3,5	1	3,5	2	3	2,53
SurfShark	1,5	4	3,5	1	2	**2,08**
ExpressVPN	1,5	2	1	5	5	3,63
PrivateVPN	5	5	2	3,5	1	3,05
Váhy kritérií	0,15	0,15	0,1	0,3	0,3	1
Povaha kritéria	MAX	MAX	MAX	MAX	MIN	

Tabulka 3 – Analýza VPN řešení, zdroj: Vlastní zpracování

Po provedení analýzy dle stanovených kritérií a vah se na prvním místě umístilo řešení od společnosti SurfShark s celkovým ohodnocením 2,08. Toto řešení nabízí masivní podporu zařízení a operačních systémů pro svou funkčnost. Dále je hlavní výhoda řešení nad konkurencí neomezený počet připojených zařízení a poměrně příznivá cena za dané řešení za rok. Řešení podporuje standardní sadu VPN protokolů (IKEv2, OpenVPN a Shadowsocks), ale ne v takové míře jako konkurenční řešení. Nevýhoda řešení je malý počet serverů, které má společnost pro funkci VPN služby, což může mít za následek pomalejší odezvy síťových služeb.

Na druhém místě se umístilo řešení od společnosti CyberGhost s ohodnocením 2,53. Řešení má poměrně slušnou podporu zařízení a operačních systémů, na kterých je možné řešení provozovat. CyberGhost má masivní infrastrukturu, ve kterém mu konkurenční řešení nemohou konkurovat. Podpora VPN protokolů (OpenVPN, IKEv2 a L2TP/IPSec) je střední, ale dostatečná. Počet najednou připojených zařízení je omezen na 7 zařízení za středně přijatelnou cenu za jeden rok. Jako jediné řešení nabízí měsíční pronájem statické IP adresy pro svá zařízení za 5 €. Vzhledem k finanční situaci a času je v nabídce velmi levné řešení na 3 roky + dva měsíce zdarma jen za 88 €. Jako jediné řešení garantuje vrácení peněz až pro 45 dní od zakoupení služby.

Třetí příčka patří řešení od společnosti PrivateVPN a to díky nízké ceně za jeden rok, vysoké podpoře VPN protokolů (OpenVPN, L2TP/IPsec, PPTP, IKEv2) a možnosti až 6 najednou připojených zařízení. Velká nevýhoda řešení je malá podpora operačních systémů (jen Windows, MacOS, iOS a Android). Další velká nevýhoda je velmi malá infrastruktura pro poskytování kvalitního VPN řešení.

Na čtvrté místě se umístilo řešení od společnosti ExpressVPN, které má masivní podporu zařízení a různých OS. Infrastruktura společnosti je na střední úrovni vzhledem k ostatním řešením. Podpora VPN protokolů je nejlepší ze všech nabízených řešení (OpenVPN, L2TP/IPSec, IKEv2/IPSec a PPTP). Společnost jako jediná nabízí neomezenou přenesou rychlost. Nevýhody řešení jsou velmi vysoká cena za rok naproti konkurenci a možnost připojení jen 5 zařízení najednou.

Poslední páté místo ve srovnání patří řešení od společnosti NordVPN. Podpora operačních systémů a zařízení je na střední úrovni. Infrastruktura společnosti je poměrně solidní, co se serverů týče, ale je provozováno jen v 57 zemích světa. VPN Protokoly mají podporu jen OpenVPN a IPSec/IKEv2. Jako jediné řešení má mimoevropské legislativní zázemí v Panamě. Cena řešení na rok je poměrně drahé s možností připojení až 6 zařízení najednou.

4.4 Analýza metod zabezpečení pro aktuální stav podniku

V kapitole 4.2 Možné metody zabezpečení sítě jsou nabízeny čtyři možnosti zabezpečení podniku (Filtrace MAC adres, RADIUS server, Proxy server a VPN), které budou v následující části zanalyzovány, a bude vybráno nejvhodnější řešení pro aktuální stav podniku. Pro analýzu byla použita metoda pořadí s váhami. Dle požadavku podniku byla stanovena kritéria (Složitost správy, Nutnost koupě dalšího HW, Míra zabezpečení a Pořizovací cena), která mají minimalizační či maximalizační povahu. Díky aktuální situaci podniku je nejdůležitějším kritériem Pořizovací cena a Složitost správy.

Analýza metod zabezpečení pro aktuální stav podniku					
Řešení	**Složitost správy**	**Nutnost koupě dalšího HW**	**Míra zabezpečení**	**Pořizovací cena**	**Součet**
Filtrace MAC adres	2	2	5	1	2,05
RADIUS/ Proxy server	4,5	4,5	3,5	4,5	4,35
VPN	2	2	3,5	3	2,63
Kombinace filtrace MAC adres a RADIUS/ Proxy server	4,5	4,5	1,5	4,5	4,05
Kombinace filtrace MAC adres a VPN	2	2	1,5	2	**1,93**
Váhy kritérií	0,25	0,2	0,15	0,4	1
Povaha kritéria	MIN	MIN	MAX	MIN	

Tabulka 4 – Analýza metod zabezpečení pro aktuální stav podniku, zdroj: Vlastní zpracování

Jako doporučené nabízené řešení pro aktuální stav podniku vyšlo dle analýzy Kombinace filtrace MAC adres a VPN s ohodnocením 1,93. Je to díky hned několika faktorům najednou. Řešení je jednoduché na správu, a tedy nemusí být přítomný IT specialista. Pro správu daného řešení bohatě stačí poučený uživatel. Není nutné dokupovat další hardware pro funkčnost řešení. Míra zabezpečení u malého podniku je na velmi dobré úrovni. Filtrace MAC adres částečně zamezí připojení se neznámým zařízením do vnitřní sítě. VPN poskytne uspokojivé zabezpečení, protože pomocí šifrovaného VPN tunelu se zvýší bezpečnost komunikace do sítě internet a pomocí VPN serveru budou uživatelé pracovat v internetu anonymně. Dále řešení umožní práci z domova, což může být poté nabízeno jako benefit. Náklady na dané řešení nejsou přehnaně vysoké, protože část, která dělá filtraci MAC adres, je již v danou dobu aktivovaná na routeru, a cena doporučené VPN služby je za dva roky provozu 69.36 €.

Druhé místo patří samotné filtraci MAC adres s ohodnocením 2,05. Režijní náklady a náklady na pořízení jsou nulové, protože filtrace je implementováno přímo na routeru. Ten je již do podniku zakoupen a daná filtrace je aktivována. Není nutnost pro svoji funkčnost dokoupení dalšího specializovaného HW. Bezpečnostní hledisko je samo o sobě nízké hlavně proto, že MAC adresy se dají jednoduše zjistit z probíhajících komunikací, např. pomocí analyzátoru paketů.

Třetí pozice patří samostatnému VPN s ohodnocením 2,63. Řešení je jednoduché na správu, není nutná koupě dalšího hardware, zabezpečení je dostatečné a cena za doporučené VPN řešení je přijatelná.

Na předposledním a posledním místě se umístila dvě řešení: Kombinace filtrace MAC adres a RADIUS/ Proxy server s ohodnocením 4,05 a RADIUS/ Proxy server s ohodnocením 4,35. I když daná řešení mají velice dobrou úroveň zabezpečení, tak jejich pořizovací cena a složitost správy je velká, a to díky části RADIUS či Proxy serveru. Pro daná řešení by se také musel pořídit samostatný HW (PC nebo server), který by funkce zastával. S tím by byla spojena i nutnost úpravy sítě a zvýšení správy daného řešení. Řešení by tedy vyžadovalo IT specialistu, což je pro podnik nyní nevýhodné.

4.5 Optimální nastavení zabezpečení sítě podniku

Pro optimální nastavení zabezpečení sítě budou využity poznatky z analytické části. Z analytické části vyplývá, že k aktuálnímu stavu podniku jsou nejoptimálnější metody zabezpečení kombinace filtrace MAC adres a VPN od poskytovatele SurfShark.

4.5.1 Popis vnitřní sítě podniku

Vnitřní síť je tvořena jako hvězdicová topologie, kde je všechna kabeláž vedena z technické místnosti. Poskytovatelem internetu je firma UPC Česká republika s.r.o., která podniku poskytla modem CBN CH7465LG. Modem sám o sobě může fungovat jako směrovač, ale pro firmu je jeho výkon a počet RJ45 výstupů nedostačující. Proto je modem přepnut do „režimu modemu“ v jeho nastavení. Na modem je připojen směrovač MikroTik RB4011iGS+5HacQ2HnD-IN, který obsahuje vstupní i výstupní firewall. Do směrovače jsou připojena všechna zařízení ve vnitřní sítí a pomocí něho spolu komunikují.

4.6 Wi-Fi router

Router MikroTik RB4011iGS+5HacQ2HnD-IN umožňuje přenos dat a informací mezi dvěma sítěmi pomocí procesu routování. Router pracuje jako bezdrátový směrovač, kde jeho hlavní činností je řídit síťový provoz. K zařízení se připojují jednotlivá bezdrátová i drátová zařízení. Směrovače od firmy MikroTik obsahují vlastní operační systém MikrotTik RouterOS postaveném na Linuxovém jádře. Do rozhraní routeru je možné se přihlásit pomocí IP adresy: 192.168.88.1. Obsahuje deset gigabitových RJ45 výstupů, které jsou plně obsaženy zařízeními v síti. Zařízení podporuje bezdrátové přenosové pásmo 2,4 GHz pro standardy IEEE 802.11b/g/n, tak i pro pásmo 5 GHz standardy IEEE 802.11a/n/ac. Pro posílení signálu router obsahuje 4x4 MIMO antény, kde každá anténa má zisk 3 dBi, vysílá do 360° a celkový výstupní výkon je až 33 dBm. Cena routeru je 4.500,- Kč bez DPH. [47]

4.6.1 Nastavení Wi-Fi sítě

Základní nastavení Wi-Fi sítě bylo změněno pro celkové zvýšení bezpečnosti a funkčnosti sítě. Jako první úprava byla změna hesla pro uživatele admin, které je v továrním nastavení bez hesla. Dále statická IP adresa routeru byla přenastavena na adresu: 192.168.1.1, která se standardně u UPC používá. Došlo k zapnutí funkce DHCP server, který přiděluje IP adresy z rozsahu 192.168.1.2 – 192.168.1.244. Byly nastaveny DNS servery, ve vlastnictví společnosti Google LLC, kterými jsou servery pod IP 8.8.8.8 a 8.8.4.4. Pro nastavení 2,4 GHz a 5 GHz sítě bylo použito zabezpečení WPA2 PSK s šifrou AES CCM. Obě bezdrátové sítě mají nastaveno adekvátní SSID a dostatečně dlouhé a složité heslo tzn. minimálně 16 znaků, obsahující číslo, nenumerický znak a alespoň jedno velké písmeno. Pro obě bezdrátové sítě byla zapnuta funkce filtrování MAC adres tak, aby se mohla připojit jen známá zařízení v rámci podniku.

4.6.2 Nastavení Firewall

Firewall pro tento router pracuje jako stavový paketový filtr. Dle jeho funkce tedy přesně definujeme, jaké síťové komunikace budou povoleny, a které zakázány – přesný princip ACL. Můžeme například zablokovat stránky se sexuálním obsahem, služby pro okamžité zasílání zpráv, nebo můžeme zakázat i celou síť s tím, že povolíme komunikace, které jsou jen nezbytně nutné. Pravidla můžeme nastavovat buď pomocí příkazové řádky anebo pomocí GUI (WinBox), které je uživatelsky přívětivější.

Malý příklad: Chceme pomocí příkazové řádky na routeru povolit WinBox na portu TCP/8291, povolit port UDP/53 pro IP: 8.8.8.8., povolit port TCP/80 a TCP/443 pro vše a zakázat vše do sítě, co není povoleno.

- /ip firewall filter add action=accept chain=input dst-port=8291 protocol=tcp comment="Povolení WinBox"
- /ip firewall filter add action=accept chain=input dst-port=53 protocol=udp src-address=8.8.8.8 comment="Povolení DNS pro specifickou IP adresu"
- /ip firewall filter add action=accept chain=input dst-port=80 protocol=tcp comment="Povolení portu 80"
- /ip firewall filter add action=accept chain=input dst-port=443 protocol=tcp comment="Povolení portu 443"
- /ip firewall filter add action=drop chain=input comment="Vše ostatní je zakázáno"

Pro implementaci firewall musí podnik přesně definovat, kam všude je nutné z vnitřní sítě přistupovat (i do ní) tak, aby stavový paketový filtr plnil svůj účel.

4.6.3 Nastavení VPN

Pro možnost využití doporučeného VPN řešení od firmy SurfShark je potřeba mít na každém zařízení nainstalovanou aplikaci SurfShark VPN. K přihlášení je nutné mít vytvořený uživatelský účet, který bude sloužit k přihlášení a k ověření zaplacené licence pro vstup k VPN serverům. Pro uživatelský účet může být nastavena i dvoufaktorová autentizace, ale to je na volbě majitele účtu. Uživatel po přihlášení může jednoduše kliknout na tlačítko „Connect“, kde bude přihlášen k doporučenému VPN serveru nebo si server může zvolit jednoduše ručně či nastavit VPN server přes statickou IP tak, aby se server nikdy nezměnil.

5 Zhodnocení a doporučení

5.1 Zhodnocení

Pro analýzy bylo podnikem stanoveno jako největší kritérium nízká cena ale tak, aby finální řešení splňovalo optimální hladina zabezpečení pro malý podnik.

Vzhledem k aktuální situaci podniku bylo po provedení analýz podniku doporučeno jako levné a efektivní řešení kombinace zabezpečení pomocí filtrace MAC adres, použití VPN, pro bezdrátové sítě použít zabezpečení WPA2 PSK s šifrou AES CCM a použití zabudovaného firewallu přímo v routeru.

Filtrace MAC adres minimalizuje možnost připojení neautorizovaného zařízení do vnitřní sítě. U malého podniku je tento typ zabezpečení velmi efektivní díky malému počtu zařízení v dané síti. Nevýhoda filtrace MAC adres je možnost odposlechnutí povolených MAC adres na úrovni paketu či fyzické odcizení povoleného zařízení do doby, než bude z povolené části filtrace odstraněno.

V rámci doporučeného řešení je zabezpečení pomocí VPN, kde hlavní výhoda spočívá ve vytvoření šifrovaného tunelu, přes který je vedena všechna komunikace mezi klientem a VPN serverem. Klient skrze VPN server komunikuje do sítě internet anonymně, protože bude vystupovat jako onen VPN server. Nevýhoda řešení spočívá v tom, že pokud spojení mezi klientem a VPN serverem spadne, tak se klient stává zranitelný pro odposlech komunikace (netýká se VPN s VPN kill-switch).

Dále bylo firmě doporučeno využití zabezpečení WPA2 PSK s šifrou AES CCM tak, aby byla každá probíhající bezdrátová komunikace skrze router šifrována.

Jako poslední bod bylo firmě doporučeno využití firewallu, který je přímo zabudovaný v routeru. Firewall funguje jako stavový paketový filtr, kde se povolují či zakazují síťové komunikace. Pro správnou implementaci firewallu do podniku je potřeba detailně rozklíčovat všechna potřebná síťová spojení ve všech směrech.

5.2 Doporučení

Pokud se podniku bude v budoucnu ekonomicky dařit, tak s tím bude spojena expanze podniku. Kvůli expanzi bude potřeba více myslet na zabezpečení dat v podnikové infrastruktuře.

Pro lepší správu a možnosti rozšíření infrastruktury bude nutné, aby podnik zainvestoval a pořídil centralizovaný switch (přepínač). Při větší infrastruktuře bude velmi náročné (nikoliv nemožné) spravovat filtraci MAC adres.

Je nutné pro podnik vytvořit interní tým IT tak, aby bylo příjemnější zázemí pro uživatele a aby IT specialisté mohli rozvíjet podnikovou infrastrukturu vzhledem k moderním bezpečnostním trendům.

Podnik bude muset zakoupit kvalitní antivirové programy přímo na klientské stanice pro zvýšení bezpečnosti, protože free verze antivirových programů nebudou stačit.

Pro zvýšení bezpečnosti bude dobré, když podnik vytvoří povinné a cyklicky se opakující e-learningová školení s testy např. na téma phishing. Následné vytvoření phishingových kampaní, které budou mít za cíl ověření znalostí uživatelů.

Doporučuje se využívat vlastní certifikační autoritu pro vytváření vlastních certifikátů a následné vynucování daných certifikátů v interní síťových komunikací a např. je nastavit jako prostředek pro připojení k Wi-Fi.

Doporučení na závěr: pravidelně vykonávat penetrační testy celkové infrastruktury podniku pro odhalení slabých míst a následně jejich vyřešení.

6 Závěr

V teoretické části byl vypracován přehled technologií bezdrátových sítí, kde jednotlivé technologie jsou rozděleny do společných kategorií dle jejich možného rozsahu. Dále byl analyzován přehled rizik a bezpečnostních opatření, která se snaží daná rizika eliminovat.

V praktické části byla provedena analýza pěti vybraných VPN poskytovatelů, kteří mají své působiště v ČR a nabízí svá řešení aspoň na jeden rok. Po provedení analýzy vyšlo pro podnik jako nejlepší možné řešení od společnosti SurfShark. Řešení je levné, poskytuje jako jediné neomezený počet najednou přihlášených zařízení a má obrovskou podporu OS a různých druhů zařízeních.

Následně bylo vytvořeno srovnání různých metod zabezpečení včetně jejich kombinací. Dle stanovených kritérií jako je Složitost správy, Nutnost koupě dalšího HW, Míra zabezpečení a Pořizovací cena bylo doporučeno řešení Kombinace filtrace MAC adres a VPN. Řešení bylo vybráno díky rozumným nákladům (není nutnost koupě dalšího HW), složitost správy řešení je minimální a míra zabezpečení je optimální pro malý podnik.

Po provedení analýz byla pro podnik vytvořena optimálně zabezpečena síť pro malý podnik, kde právě byly využity všechny poznatky, které byly v analýzách uvedeny.

Jednu z pochopitelných chyb, které podnik dělá, vzhledem k aktuální situaci je, že podnik upřednostňuje finance před bezpečností síťové infrastruktury. Osobně bych spíše upřednostňoval bezpečnost před nízkými náklady, anebo udělal nějaký logický kompromis mezi těmito dvěma kritérii. Podnik si musí uvědomit, že pracuje s citlivými uživatelskými daty a že každé odcizení dat může být pro podnik likvidační. Podniku při odcizení hrozí zákaz činnosti či udělení přestupku dle Zákona č. 110/2019 Sb. - Zákon o zpracování osobních údajů, kde výše přestupku pro právnické osoby může dosahovat až do výše 10.000.000,- Kč.

Podnik musí aktivně sledovat a uplatňovat bezpečnostní trendy. Aktuálně zabezpečená síť je vždy jen do té doby, než bude jednoduše prolomitelná. Riziko prolomitelnosti technologie se vždy zvyšuje časem, po který se daná technologie používá nebo samotným vstupem novějších technologií na globální trh a samozřejmě celkově i vzdělanost lidí v oblasti informačních technologií.

Při budoucím studiu navazujícího magisterského programu může být bakalářská práce využita jako podklad pro sepsání mé diplomové práce, neboť bezpečnostní technologie

mohou být rozebrány do větších podrobností včetně vytvoření sofistikovanější a bezpečnější podnikové infrastruktury.

Bakalářská práce může sloužit jako podklad pro vybudování bezpečné infrastruktury menšího podniku s doporučením i pro budoucí vývoj růstu podniku.

7 Seznam použitých zdrojů

1. DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP: Bezpečnost. Brno: Computer Press, 2001. 566 s. ISBN 80-7226-513-X.
2. NORTHCUTT, Stephen, ZELTSER, Lenny, WINTERS, Scott, FREDERICK, Karen Kent, RITCHEY, Ronald W. Bezpečnost počítačových sítí: Kompletní průvodce návrhem, implementací a údržbou zabezpečené sítě. Brno: Computer Press, 2005. 592 s. ISBN 80-251-0697-7.
3. SCAMBRAY, Joel, MCCLURE, Stuart, KURTZ, George. Hacking bez tajemství, 2. aktualizované vydání. Brno: Computer Press, 2002. 626 s. ISBN 80-7226-644-6.
4. SOSINSKY, Barrie A. Mistrovství - počítačové sítě: vše, co potřebujete vědět o správě sítí. Brno: Computer Press, 2010. 840 s. ISBN 978-80-251-3363-7.
5. ZANDL, Patrick. Bezdrátové sítě WiFi: praktický průvodce. Brno: Computer Press, 2003. 190 s. ISBN 80-7226-632-2.
6. DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.
7. MANAGEMENTMANIA.COM. Počítačová síť (Computer network). [Online]. [cit. 06.07.2019]. Dostupné z WWW: https://managementmania.com/cs/pocitacova-sit
8. KYSELA, Jiří. Bezdrátový Internet a technologie Wi-Fi v České republice. [Online]. [cit.06.07.2019]. Dostupné z WWW: http://www.internetprovsechny.cz/bezdratovy-internet-a-technologie-wi-fi-v-ceske-republice/
9. FREEWIMAXINFO.COM. What is Wireless network – Types – WLAN, WiFi, WMAN & Wireless Technologies. [Online]. [cit. 06.07.2019]. Dostupné z WWW: http://freewimaxinfo.com/wireless-network.html
10. CTU.CZ. Využívání vymezených rádiových kmitočtů. [Online]. [cit. 07.07.2019]. Dostupné z WWW: https://www.ctu.cz/vyuzivani-vymezenych-radiovych-kmitoctu
11. OPENSIGNAL.COM. The State of LTE(February 2018) [Online]. [cit. 07.07.2019]. Dostupné z WWW: https://www.opensignal.com/reports/2018/02/state-of-lte
12. KAVANAGH, Sacha. How fast is 5G?. [Online]. [cit. 07.07.2019]. Dostupné z WWW: https://5g.co.uk/guides/how-fast-is-5g/
13. STOP5G.CZ. Škodlivé účinky 5G. [Online]. [cit. 07.07.2019]. Dostupné z WWW: https://stop5g.cz/
14. VÁCLAVÍK, Luláš. Historie Wi-Fi se začala psát před 25 lety. Připomeňte si hlavní milníky [Online]. [cit. 13.07.2019]. Dostupné z WWW: https://www.cnews.cz/historie-wi-fi-se-zacala-psat-pred-25-lety-pripomente-si-hlavni-milniky/
15. WI-FI.UNAS.CZ. IEEE 802.11. [Online]. [cit. 13.07.2019]. Dostupné z WWW: http://wi-fi.unas.cz/ieee-802-11.php
16. SIMANDL, Martin. IEEE 802.11n — Jak na rychlé Wi-Fi doma i venku. [Online]. [cit. 13.07.2019]. Dostupné z WWW: https://pctuning.tyden.cz/hardware/site-a-internet/16921-ieee-802-11n-jak-na-rychle-wi-fi-doma-i-venku?start=1

17. PRAVDA, Ivan. Přehled doplňků standardu IEEE 802.11. [Online]. [cit. 14.07.2019] Dostupné z WWW: http://access.feld.cvut.cz/view.php?cisloclanku=2005113002
18. HOME-NETWORK-HELP.COM. 802.11 Wireless Standard. [Online]. [cit. 14.07.2019] Dostupné z WWW: https://www.home-network-help.com/802-11.html
19. KVALITNI-INTERNET.CZ. Závratná rychlost, vysoký výkon a velká odolnost proti rušení. Nový WiFi standard IEEE 802.11ax je tady. [Online]. [cit. 21.07.2019]. Dostupné z WWW: https://kvalitni-internet.cz/zavratna-rychlost-vysoky-vykon-velka-odolnost-proti-ruseni-novy-wifi-standard-ieee-80211ax-je-tady
20. HOFFMAN, Chris. What's the Difference Between Ad-Hoc and Infrastructure Mode WiFi?. [Online]. [cit. 28.07.2019]. Dostupné z WWW: https://www.howtogeek.com/180649/htg-explains-whats-the-difference-between-ad-hoc-and-infrastructure-mode/
21. TETZ, Edward. Wireless Networking Infrastructure Mode. [Online]. [cit. 28.07.2019]. Dostupné z WWW: https://www.dummies.com/programming/networking/cisco/wireless-networking-infrastructure-mode/
22. MAN-IN-THE-MIDDLE.CZ. Man in the middle: nestaňte se obětí podvodníků. [Online]. [cit. 28.07.2019]. Dostupné z WWW: https://www.man-in-the-middle.cz/
23. HACKINGKURZY.CZ. Brute force – útok na hesla hrubou silou. [Online]. [cit. 11.08.2019]. Dostupné z WWW: https://www.hackingkurzy.cz/blog/brute-force-utok-na-hesla-hrubou-silou/
24. GOVCERT.CZ. SOCIÁLNÍ INŽENÝRSTVÍ. [Online]. [cit. 11.08.2019]. Dostupné z WWW: https://www.govcert.cz/cs/informacni-servis/doporuceni/2486-socialni-inzenyrstvi/
25. US.NORTON.COM. What is the Difference Between Black, White and Grey Hat Hackers?. [Online]. [cit. 18.08.2019]. Dostupné z WWW: https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html
26. WEBSERVER.ICS.MUNI.CZ. Bezpečnostní funkce v počítačových sítích. [Online]. [cit. 15.09.2019]. Dostupné z WWW: http://webserver.ics.muni.cz/bulletin/articles/171.html
27. SMIRNOFF, Peter, TURNER, Dawn M. Symmetric Key Encryption - why, where and how it's used in banking. [Online]. [cit. 15.09.2019]. Dostupné z WWW: https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking
28. SSL2BUY.COM. Symmetric vs. Asymmetric Encryption – What are differences?. [Online]. [cit. 15.09.2019]. Dostupné z WWW: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences
29. ROUSE, Margaret. 802.11i. [Online]. [cit. 05.10.2019]. Dostupné z WWW: https://searchmobilecomputing.techtarget.com/definition/80211i
30. FLYLIB.COM. Robust Security Network (RSN) Operations. [Online]. [cit. 05.10.2019]. Dostupné z WWW: https://flylib.com/books/en/2.519.1/robust_security_network_rsn_operations.html

31. KRČMÁŘ, Petr. Šifrování WPA2 prolomeno, Wi-Fi sítě je možné odposlouchávat (aktualizováno). [Online]. [cit. 05.10.2019]. Dostupné z WWW: https://www.root.cz/clanky/sifrovani-wpa2-bylo-prolomeno-wi-fi-site-je-mozne-odposlouchavat/
32. WIFI.ORG. Security [Online]. [cit. 06.10.2019]. Dostupné z WWW: https://www.wi-fi.org/discover-wi-fi/security
33. BELOŠA, Ingrid. Understanding Access Control Lists (ACL) [Online]. [cit. 26.10. 2019]. Dostupné z WWW: https://www.routerfreak.com/understanding-access-control-lists-acl/
34. EMPEY, Charlotte. Co je VPN a jak funguje? Váš základní průvodce. [Online]. [cit. 27.10.2019]. Dostupné z WWW: https://blog.avast.com/cs/co-je-vpn-a-jak-funguje
35. NEJLEPSIVPN.CZ. Srovnání: Protokoly VPN – Který nastavit?. [Online]. [cit. 27.10.2019]. Dostupné z WWW: https://www.nejlepsivpn.cz/protokoly-vpn/
36. OTOUPALÍK, Petr. Princip zabezpečení protokolovou sadou IPsec. [Online]. [cit. 27.10.2019]. Dostupné z WWW: http://realtimesecure.asp2.cz/ipsec.aspx
37. OPENVPN.NET. Commercial VPN server Resources. [Online]. [cit. 27.10.2019]. Dostupné z WWW: https://openvpn.net/vpn-server-resources/
38. ANTIVIROVECENTRUM.CZ. Softwarové Firewally [Online]. [cit. 27.10.2019]. Dostupné z WWW: https://www.antivirovecentrum.cz/firewally.aspx
39. IBM.COM. Přehled o protokolu RADIUS (Remote Authentication Dial In User Service) [Online]. [cit. 22.01.2020]. Dostupné z WWW: https://www.ibm.com/support/knowledgecenter/cs/ssw_ibm_i_72/rzaiy/rzaiyradiusovw.htm
40. WEBSERVER.ICS.MUNI.CZ. 802.1X – autentizace v počítačových sítích [Online]. [cit. 22.01.2020]. Dostupné z WWW: http://webserver.ics.muni.cz/bulletin/articles/590.html
41. THESECURITYBUDDY.COM. What is a Proxy Server and how does it work ? [Online]. [cit. 25.01.2020]. Dostupné z WWW: https://www.thesecuritybuddy.com/network-security/what-is-a-proxy-server-and-how-does-it-work/
42. NORDVPN.COM. [Online]. [cit. 29.01.2020]. Dostupné z WWW: https://nordvpn.com/
43. CYBERGHOSTVPN.COM. [Online]. [cit. 29.01.2020]. Dostupné z WWW: https://www.cyberghostvpn.com/en_US/
44. SURFSHARK.COM. [Online]. [cit. 29.01.2020]. Dostupné z WWW: https://surfshark.com/
45. EXPRESSVPN.COM. [Online]. [cit. 29.01.2020]. Dostupné z WWW: https://www.expressvpn.com/
46. PRIVATEVPN.COM. [Online]. [cit. 29.01.2020]. Dostupné z WWW: https://privatevpn.com/
47. I.MT.LV. THE 4011 SERIES [Online]. [cit. 30.01.2020]. Dostupné z WWW: https://i.mt.lv/cdn/rb_files/RB4011-IN-180919132356.pdf