Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Budování a využívání menších počítačových sítí

Jiří Borecký

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jiří Borecký

Systémové inženýrství a informatika
Informatika

Název práce

Budování a využívání menších počítačových sítí

Název anglicky

Construction and use of smaller computer networks

Cíle práce

Cílem práce je vybudování, instalace a provoz menší počítačové sítě, která bude sloužit firemním účelům. Dalším cílem je zhodnocení přínosu navrženého, realizovaného a otestovaného řešení.

Vyhodnocení bude provedeno na základě výsledků testů dostupnosti celé počítačové sítě, dílčích testů připojení k internetu a též, zda-li probíhá bezproblémová komunikace mezi dvěma kancelářemi, či nikoli.

Metodika

Metodika bakalářské práce je založena na analýze odborných a vědeckých dokumentů (zejména monografií) a následně budou získané poznatky synteticky využity návrhové části. Postupujte dle následujících bodů:

- Navrhněte a vybudujte počítačovou síť pro menší (do 200 zaměstnanců) firmu
- Zhodnoťte přínosnost navrženého řešení oproti bežně používaným (WiFi versus Ethernet atd)
- Řešení otestujte
- Definujte závěry

Doporučený rozsah práce

30-40

Klíčová slova

VPN (Virtual Private Network), zálohování, počítačová síť

Doporučené zdroje informací

ELENKOV, N. Android securityinternals. 1. vydání, San Francisco : NoStarchPress, Inc., 2015. 407 s. ISBN 978-1-59327-581-5

KAKADIA, D., BRABSTON, M. E., DIMABRO, F. Networking Concepts and Technology. 1. vydání, US : Pearson Education, 2007. 388 s. ISBN 0131482076

MERKOW, M. S. Virtual Private Networks for Dummies. 1. vydání, US : For Dummies, 1999. 346 s. ISBN 9780764505904

Předběžný termín obhajoby

2020/21 LS – PEF

Vedoucí práce

Ing. Josef Pavlíček, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 23. 2. 2021

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 23. 2. 2021

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 25. 02. 2021

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Budování a využívání menších počítačových sítí" jsem vypracoval(a) samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.3.2021 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Josefu Pavlíčkovi, Ph.D. za odborné vedení mé bakalářské práce, za cenné připomínky, ochotné a pečlivé čtení tohoto textu. Všechny připomínky výrazně pomohly k doplnění a zlepšení mé práce. Velké poděkování patří i mé rodině, vždy mě podporovali, jak při psaní této práce, tak též v celém průběhu studia.

Budování a využívání menších počítačových sítí

Abstrakt

Tato bakalářská práce řeší vybudování, instalaci a provoz menší počítačové sítě, která slouží k firemním účelům. Cílem bylo zhodnotit přínosy navrženého, realizovaného a otestovaného řešení. Vyhodnocení proběhlo na základě výsledků testů dostupnosti celé počítačové sítě, dílčích testů připojení k internetu a také bezproblémové komunikace mezi dvěma vzdálenými kancelářemi, které jsou součástí jedné sítě. V závěru jsou formulovány konkrétní realizované kroky vedoucí ke snazší komunikaci mezi zařízeními v jednotlivých kancelářích a lepší bezpečnosti uložených dat i mobilních zařízení.

Klíčová slova: VPN (Virtual Private Network), zálohování, počítačová síť

Construction and use of smaller computer networks

Abstract

This thesis deals with the construction, instalation and operation of a smaller computer network, which is used for corporate purposes. The aim was to evaluate the benefits of the proposed, implemented and tested solution. The evaluation was based on the results of tests of the availability of the entire computer network, partial tests of the Internet connection, seamless communication between two remote offices that are part of one network. In the end, specific implemented steps are formulated leading to easier communication between devices in individual offices and better data and mobile devices security.

Keywords: VPN (Virtual Private Network), backup, computer network

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSL	Digital Subscriber Line
GB	Gigabyte
GPS	Global Positioning System
ICMP	Internet Control Message Protocol
IP	Internet Protocol
MAC	Media Access Control
MB	Megabyte
OS	Operation System
PC	Personal Computer
PDF	Portable Document Format
PIN	Personal Identification Number
RDP	Remote Desktop Protocol
SIM	Subscriber Identity Module
SMS	Smart Message
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
VA	Volt-ampere
VPN	Virtual Private Network
W	Watt
Wi-Fi	Wireless-Fidelity

Úvod

Měj odvahu
aby hluk ostatních názorů
nepřekřičel tvůj vlastní vnitřní hlas.
Steve Jobs,[1]

Představme si slovo počítačová síť, člověk ho může všedně označit za běžné slovo, vyskytující se velmi často v našem okolí. Ve skutečnosti si už dnešní svět bez počítačových sítí a síťového připojení nedokážeme ani představit.

Dnes již naprostá většina domácností vlastní internetové připojení. Využívá jej jak pro běžné pobavení a odreagování se, tak i pro další účely. Bez internetu by zcela jistě nemohl vzrůstat trend tzv. chytrých zařízení, jako jsou například telefony, televize, ale také i inteligentní budovy. Připojení k internetu a počítačových sítí dále využívají i restaurace a kavárny, ve kterých je možné se připojit přes Wi-Fi. Osobně ovšem doporučuji se připojit přes VPN (virtuální privátní síť) z důvodu možného hackerského útoku (konkrétně se nazývá „Man-in-the-middle“) osoby, která je taktéž připojená ke stejné (mnohdy nezabezpečené) síti. Tou osobou může být nenápadný návštěvník, který sedí o dva stoly vedle nás. Pokud se připojíme přes VPN, znemožníme tak naslouchání síťové komunikace našeho zařízení.

Nyní se dostáváme na místa, kde počítačová síť a internetové připojení je nutností. Tím jsou místa v zaměstnání a kanceláře. Dokázali bychom si představit zaměstnání bez počítačové sítě? V dnešní době již málokdo si dokáže přestavit takovou skutečnost. Počítače ve firmách, ať už jsou firmy velké či malé, bývají propojeny do jedné centrální sítě, která je třeba v jiné zemi, či v jiném státě. Dokážeme si přestavit život bez počítačů? Slýcháváme teorie, které praví, že bez počítačů a sítí bylo lépe. Tuto otázku si ovšem musí každý zodpovědět sám.

1 Cíl práce a metodika

1.1 Cíl práce

Cílem práce je vybudování, instalace a provoz menší počítačové sítě, která bude sloužit firemním účelům. Hlavním oborem konkrétní firmy je vedení účetnictví. Jelikož účetní data, daně a mzdová problematika v sobě skrývá citlivá data, je velmi důležité takovou počítačovou síť dobře zabezpečit a poskytnout jí rychlé a spolehlivé připojení k internetu.

Zpočátku je popsána charakteristika počítačové sítě, obsahující popis místa, účelu a přehledně zobrazující použitá zařízení, které se do sítě připojují. Zařízení jsou zobrazena v logických i fyzických schématech. Následně se práce věnuje analýze současného (tzv. AS-IS) stavu, který je zhodnocen z pohledu přenosové rychlosti, jak spolu zařízení komunikují a jaké jsou jejich požadavky, celkový stav a zdraví sítě i rychlosti odezvy. Dále je také zhodnocena bezpečnost sítě, její ochrana vůči virům a také ochrana dalších přenosných zařízení, která jsou do sítě zainteresována.

Dalším cílem je návrh nového řešení, které by uspokojilo nejen potřeby uživatelů, ale také, aby bylo zohledněno zabezpečení dat a celé sítě. Navrhované řešení obsahuje antivirové programové vybavení, které zvyšuje bezpečnost sítě včetně připojených mobilních zařízení. Ve výsledku by navržené řešení mělo propojit dvě lokální sítě do jedné a bezproblémově využít síťové služby.

Následuje zhodnocení přínosu tohoto navrženého, realizovaného a otestovaného řešení, které bude provedeno na základě výsledků testů dostupnosti celé počítačové sítě, dílčích testů připojení k internetu a též, zdali probíhá bezproblémová komunikace mezi dvěma kancelářemi, či nikoli.

1.2 Metodika

Metodika bakalářské práce je založena na analýze odborných a vědeckých dokumentů (zejména monografií) a následně budou získané poznatky synteticky využity návrhové části. Postupujte dle následujících bodů:

- Navrhněte a vybudujte počítačovou síť pro menší (do 200 zaměstnanců) firmu
- Zhodnoťte přínosnost navrženého řešení oproti běžně používaným (WiFi versus Ethernet atd)
- Řešení otestujte
- Definujte závěry

2 Současný stav poznání řešené problematiky

2.1 Popis místa

Realizace počítačové sítě je v panelovém domě v Praze. Síť se dělí na dvě kanceláře, které jsou vzdušnou čarou od sebe vzdálené asi 75 metrů. Každá kancelář představuje bytovou jednotku, ve které je provozována lokální počítačová síť. V současné chvíli nejsou zařízení mezi kancelářemi nijak propojeny a jsou pouze samostatně lokálními zařízeními v každé kanceláři zvlášť. Cílem práce je navrhnout řešení pro sdílené propojení počítačů a ostatních zařízení do jedné privátní sítě. Síť využívají dvě fyzické osoby (podnikatelé) k externímu vedení účetnictví, zpracování daní a mezd zaměstnanců. Dalšími uživateli sítě jsou návštěvy, klienti (kteří dorazí na konzultaci) a také správce sítě. Všichni využívají bezdrátové připojení přes Wi-Fi.

Pomocí ethernetového kabelu jsou připojeny stolní počítače, které běží na operačních systémech Microsoft – verze Windows 7 a 10. Dalšími systémy zainteresovanými do sítě, které využívají především klienti a návštěvy na mobilních zařízení, jsou Android, Windows mobile a iOS.

Pro lepší představu, jak jsou od sebe vzdáleny a rozmístěny kanceláře, je zde zobrazen letecký družicový snímek, který poskytuje společnost Google v jejich Google Earth aplikaci.

Obr. 1 Letecký pohled

2.1.1 Poskytovatel připojení

Připojení poskytuje společnost UPC, která nabízí kabelové připojení. Poskytovatel byl vybrán z důvodu stabilního a velice rychlého připojení k internetu a jeho dobrého jména. Realita ovšem může být trochu jiná, než se může na první dojem zdát, jelikož občas v měsíci nastávají výpadky služeb ze strany poskytovatele UPC. Jedná se spíše o krátkodobé výpadky, nicméně není příjemné zjistit, že se najednou nestahují, případně neodesílají data. Dalším příkladem může být situace, kdy se vyplní dlouhý formulář a při odesílání se zjistí, že jednoduše nelze odeslat z důvodu nedostupných služeb. Je velmi obtížné zachovat klid a nepropadat panice.
Na druhou stranu společnost UPC nabízí rychlé připojení k internetu, což je velmi výhodné. V současné chvíli mají v nabídce rychlosti připojení od 50 Mb/s až po 1 Gb/s.[2]

2.2 Kancelář 1

První kancelář se nachází ve třetím patře panelového domu. Rozdělení kanceláře je řešené na 3 místnosti s kuchyní a koupelnou. V hlavní pracovně se nachází kabelový DSL modem, který převádí analogový signál na digitální. Použití je zde podmíněno především z důvodu telefonního připojení, které je standardně propojeno ethernetovým kabelem RJ-11.
K tomuto modemu je připojen router (směrovač) pomocí kabelu RJ-45, který představuje v síti velmi důležitou pozici. Použil jsem označení pro tento router RT-1. Router plní funkci tzv. „centrální mozku sítě“. Proto je třeba brát ohled na jeho pečlivý výběr. Mezi jeho hlavní parametr patří rychlé „routování“, což znamená směrování požadavků po síti. Jako příklad můžeme uvést zobrazení webové stránky. Koncový uživatel pracující na zařízení v síti vyšle požadavek na webový server: „zobraz obsah webové stránky“ a tento server uživateli odpoví. Resp. přesněji řečeno všechny požadavky jdou právě přes router, který dotazy třídí a rozesílá na správná místa. Taktéž odpovědi, což v našem popsaném případě je právě odpověď na dotaz zobrazení webové stránky. Ve skutečnosti je to totiž router, který dostane odpověď od webového serveru a tuto odpověď pošle na zdrojové zařízení, které o ni zažádalo. Z důvodu potřeby taktéž bezdrátového přenesu byl pořízen Wi-Fi router, na který se lze připojit z kteréhokoli místa v kanceláři. Abychom se mohli dobře připojit z libovolného místa v kanceláři, potřebujeme anténu se silným zesílením signálu. Zabezpečení sítě vyžaduje zadání hesla, při pokusu o připojení k síti, není tedy možné se připojit bez znalosti hesla.

K routeru se přes síťový kabel připojuje tiskový server (USB print server – označený PS-1). Jedná se o neveliké zařízení, které umožňuje připojení k laserové tiskárně LT-1 a to z kteréhokoli zařízení v síti podporující tisk úloh. Má přiřazenou pevnou IP adresu, jejíž rezervaci zajišťuje DHCP server, který je součástí routeru. Tato adresa je zcela účelně nastavená jako neměnná, aby nedocházelo k problémům s připojením k tiskárně nebo k zamezení problémům s nedostupností tiskárny.

Dalším klíčovým zařízením je stolní počítač, jedná se o hlavní pracovní stanici, která je označena jako PC-1. K routeru je připojen pomocí UTP ethernetového kabelu kategorie 5e. IP adresa síťové karty je na tomto počítači také rezervována pomocí DHCP serveru a to z důvodu, který bude popsán dále.

Ke stolnímu počítači PC-1 je připojena multifunkční laserová tiskárna LT-2 pomocí USB kabelu. Tiskárna se může pochlubit dalšími funkcemi kromě tisku, a sice umožňuje kopírování a skenování, které je také silně využíváno a vyžadováno. V tomto případě se neřešilo pevné přidělení IP adresy, protože tiskárna slouží především ke kopírování, které není v současné chvíli využíváno více uživateli.

Pocit odpočinku a relaxace vytváří „smart“ televize, která je do sítě připojena ethernetovým kabelem. Jedná se o tzv. chytrou televizi umožňující sledovat filmy uložené na síťovém úložišti nebo procházení videí na Youtube.com. V současné chvíli je připojení do sítě využíváno právě pro prohlížení Youtube videí. Síťový disk není nastaven ani nainstalován. Filmy lze prohlížet i přes USB disk, který je možný připojit přímo do televize.

Pro ucelený přehled zařízení využívající počítačovou síť, nesmí chybět mobilní telefon. Mobily se připojují přes bezdrátové Wi-Fi připojení. Připojení se využívá hlavně pro stahování aktualizací v telefonu, aby se zbytečně nečerpala data poskytnutá mobilním operátorem. Aktualizační balíčky obsahují stále více a více dat, proto je výhodné se připojovat k Wi-Fi namísto plýtvat data od mobilního operátora. Běžně jsou do sítě připojeny telefony MB-1 a MB-2, v případě návštěvy se připojují další zařízení označeny OZ.

V neposlední řadě jsou bezdrátově připojeny dva notebooky. Na prvním notebooku NB-1, který je převážně umístěný v místnosti LO, je často využívána služba RDP (připojení ke vzdálené ploše) na PC-1 z důvodu snadné dostupnosti dat. Odezva a její rychlost je uspokojivá.

2.2.1 Přehled zařízení v kanceláři 1

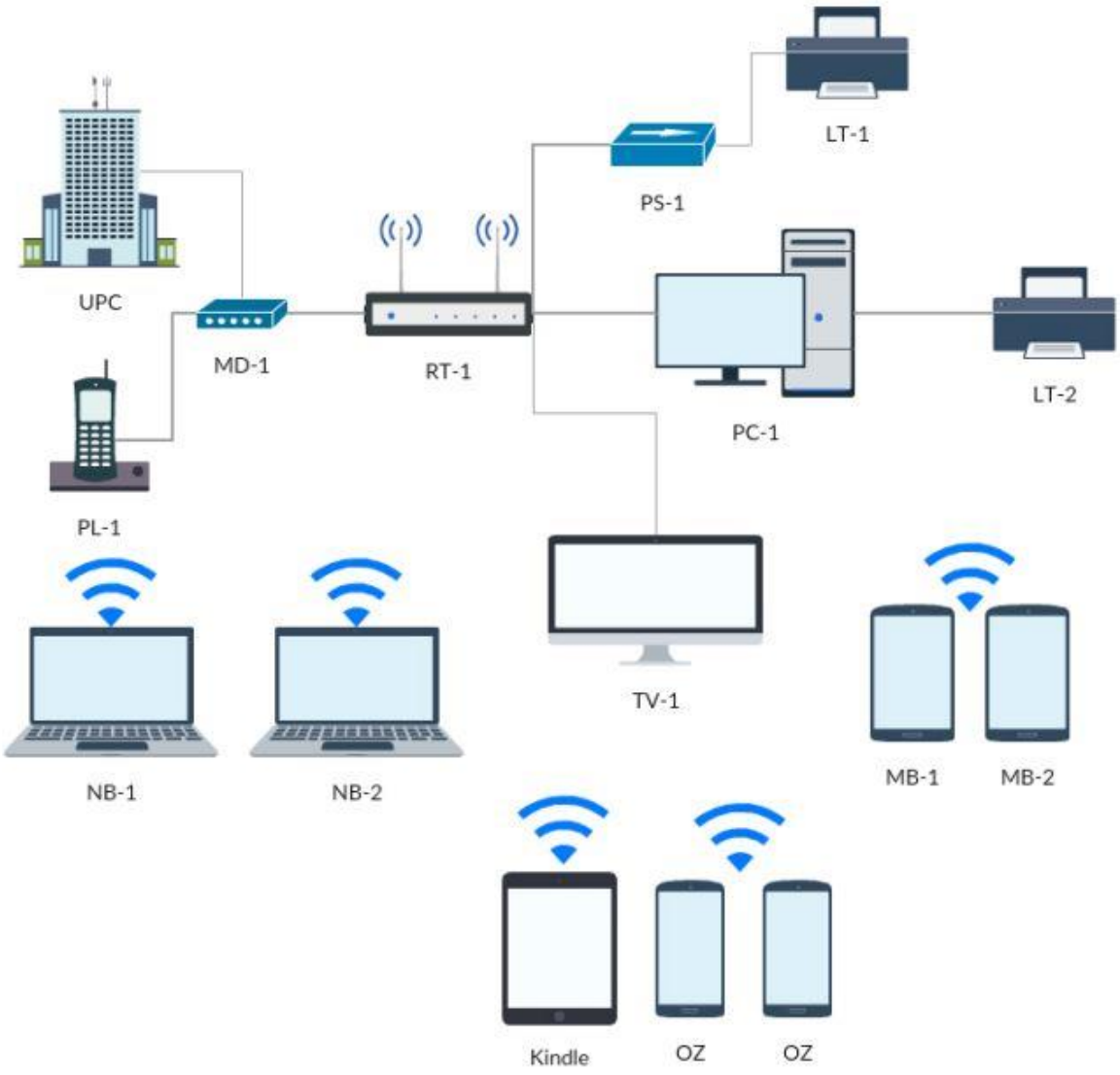
Pro přehlednost a jednoduchý popis každého zařízení, které je umístěné v síti, je využito zobrazení v tabulce. Syntaxe je následující: velkými písmeny jsou napsány první písmena názvu zařízení, následuje pomlčka a číslice. Nastane-li případ, kdy podobných zařízení je více, je jim postupně přiřazeno vyšší následující číslo. Stejně je to se zápisem umístění. Např. laserová tiskárna HP LJ P2055 je označena LT-1 (jedná se o tiskárnu s pořadovým číslem 1) a je umístěna v místnosti označené jako OB. Ostatní zařízení jsou shrnuta do označení OZ, jejich umístění je zapsáno jako PZ (přenosná zařízení). Tyto zařízení využívají především klienti nebo návštěvy, kteří si s sebou přinesou mobilní telefon či tablet. Pokud se totiž chtějí připojit do sítě, musí se připojit na bezdrátový router pomocí Wi-Fi technologie a po zadání hesla je možné se přidat do sítě.

Tab. 1 Přehled zařízení v kanceláři 1

Název zařízení	Označení	Umístění
Modem Cisco EPC3208	MD-1	OB
Bezdrátový router TP-Link TL-WE841ND	RT-1	OB
Pevná linka Panasonic KX-TG6421FX	PL-1	OB
USB Print server NETGEAR PS121	PS-1	OB
Laser tiskárna HP LJ P2055	LT-1	OB
Laser tiskárna HP LJ M1132	LT-2	OB
Smart TV Philips 32PFL3517H/12 (LAN)	TV-1	OB
Stolní PC	PC-1	OB
Notebook Asus EEE	NB-1	LO
Notebook Lenovo X220	NB-2	PO
Mobilní telefon 1	MB-1	PZ
Mobilní telefon 2	MB-2	PZ
Čtečka Amazon Kindle	EČ-1	PZ
Ostatní zařízení návštěvy	OZ	PZ

2.2.2 Topologie s diagramem sítě kanceláře 1

Na následujícím obrázku je možno vidět rozložení topologie a diagram sítě v kanceláři 1. Toto schéma bylo vytvořeno aplikací Creately. [3]



Obr. 2 Topologie s diagramem sítě kanceláře 1

2.2.3 Schéma adresace v kanceláři 1

Přidělení IP adresy ke konkrétnímu zařízení je zajištěné DHCP serverem, který běží na routeru RT-1. Rozsah přidělovaných IP adres je nastavena na 192.168.1.102 – 192.168.1.120, tzn. pro 19 zařízení. Není problém daný rozsah upravovat přes webovou administraci (webové rozhraní routeru, na kterém běží DHCP server). Jedná se o webovou stránku, na kterou se lze připojit libovolným zařízením v síti, po napsání adresy výchozí brány sítě do webového prohlížeče je požadováno přihlašovací jméno a heslo, které je známé pouze správci sítě. Adresa výchozí brány je 192.168.1.1.

DHCP server provádí přiřazení IP adresy buď dynamicky nebo podle DHCP rezervace (jedná se o tabulku). Pokud chceme provést rezervaci IP adresy konkrétního zařízení, je potřebné vědět tzv. MAC adresu (jedná se o fyzické označení síťové karty). Při připojení zařízení do počítačové sítě je prohledána tabulka DHCP rezervace. Pokud se zde zařízení vyskytuje, je mu přiřazena konkrétní IP adresa. Pokud ne, je mu přiřazena IP adresa dle volných míst v daném rozsahu.

Tab. 2 Schéma adresace kancelář 1

Označení	Přiřazení IP adresy	IP adresa	Výchozí brána	Maska sítě
RT-1	Staticky	192.168.1.1	-	255.255.255.0
PS-1	DHCP rezervace	192.168.1.104	192.168.1.1	255.255.255.0
PC-1	DHCP rezervace	192.168.1.102	192.168.1.1	255.255.255.0
TV-1	DHCP	-	192.168.1.1	255.255.255.0
NB-1	DHCP	-	192.168.1.1	255.255.255.0
NB-2	DHCP	-	192.168.1.1	255.255.255.0
MB-1	DHCP	-	192.168.1.1	255.255.255.0
MB-2	DHCP	-	192.168.1.1	255.255.255.0
OZ	DHCP	-	192.168.1.1	255.255.255.0

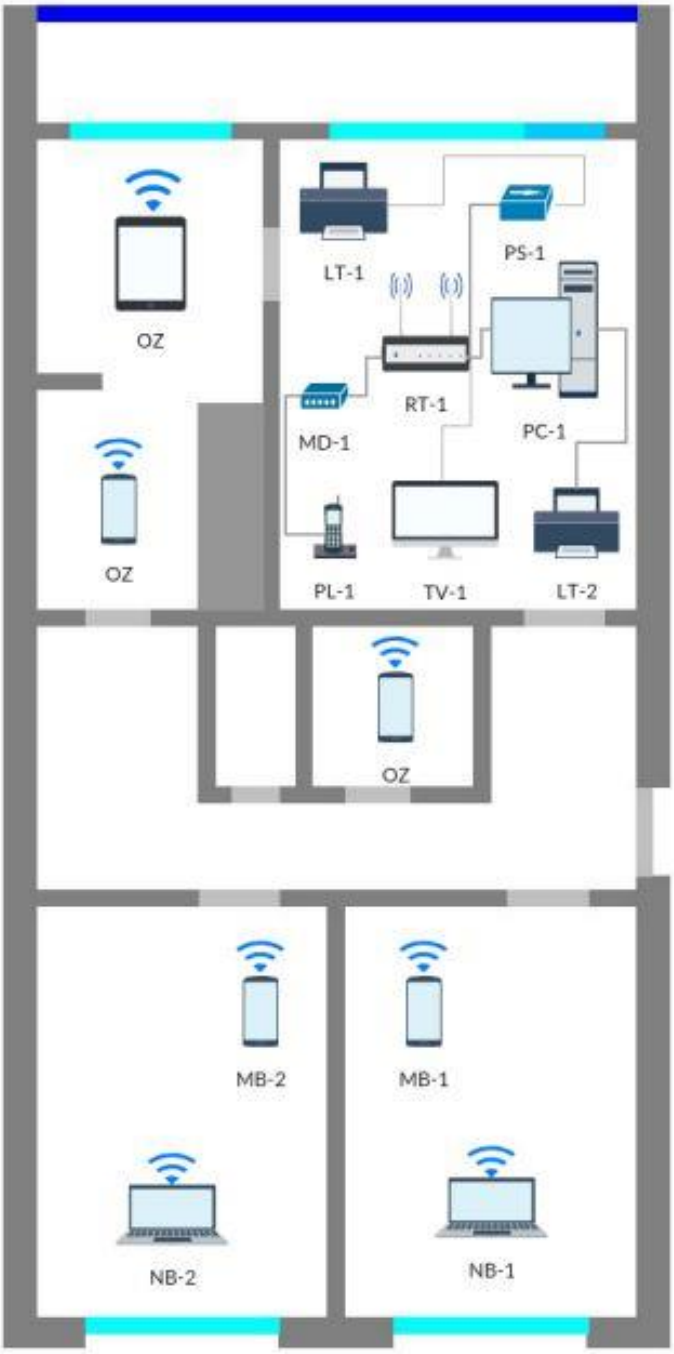
Jako první zarezervované zařízení je print server (který má označení PS-1), tomuto print serveru je přiřazena IP adresa pomocí DHCP rezervace. Tedy pro správnou funkci je nutné přiřadit zařízení konkrétní IP adresu a sice 192.168.1.104. Kdyby se nevytvořila rezervace adresy, tiskárna by mohla být nedostupná a nebylo by možné provádět tisk a zařízení by mezi sebou neměli možnost komunikovat.

Druhým zařízením, které má rezervovanou IP adresu je stolní počítač (který je označený PC-1). Zde je důvodem aplikace Form Studio, která je na počítači nainstalovaná. Tento program slouží pro tvorbu formulářů. Smysl rezervace IP adresy v tomto případě je takový, že můžeme nastavit jeden počítač jako server, který má uložená data a další zařízení jako klienti, kteří se připojují na tento server a čtou z něj potřebná data. Formuláře se tak ukládají na stejné místo, ke kterému se lze připojit z více zařízení. Provedené nastavení je zde ponecháno z předchozích důvodů, kdy docházelo ke každodennímu připojení dvou počítačů k jednomu datovému úložišti na konkrétní IP adresu 192.168.1.102. V současnosti se data sdílí fyzicky přes USB flash disk nebo přes Google Disk úložiště a to právě z důvodu, že kanceláře nejsou nijak propojeny.

Další sítová zařízení mají IP adresy přiřazené dynamicky. Jedná se o zařízení TV-1, což představuje smart televizi, dva notebooky NB-1 a NB-2, MB-1 a MB-2 jsou označeny mobilní telefony a OZ jsou označeny ostatní zařízení.

2.2.4 Grafické schéma kanceláře 1

Schéma zobrazuje místnosti a v nich rozmístění jednotlivých zařízení. Podlaží je vysoké 2,9 m, nosné konstrukce jsou z betonových panelů o tloušťce 19 cm a železobetonové příčky mají tloušťku 6 cm. Bytové jádro je z konstrukce se stěnami ze sololitu a jádra z lisovaného papíru.[4]



Obr. 3 Grafické rozložení kanceláře 1

Následující tabulka přehledně zobrazuje rozměry jednotlivých místností v m^2, které již byly znázorněny v grafickém rozložení.

Tab. 3 Výměry místností kancelář 1

Místnost	Výměra
Kuchyň	10,92 m^2
Pokoj 1 (OB)	18,30 m^2
Pokoj 2 (PO)	11,48 m^2
Pokoj 3 (LO)	11,48 m^2
Předsíň	13,41 m^2
Koupelna	3,30 m^2
WC	1,93 m^2
Lodžie	6,18 m^2
Sklep	1,50 m^2
Celkem plochy	78,50 m^2

2.3 Kancelář 2

Druhá kancelář se nachází v prvním patře panelového domu. Skládá se ze dvou místností s koupelnou a kuchyní.

V kanceláři bylo požadováno zajistit bezdrátové připojení k síti, proto zde nejsou žádné síťové kabely. Přenos dat funguje bez větších problémů, nejedná se o velký prostor, a proto zde není problém s pokrytím signálem Wi-Fi.

Nachází se zde bezdrátový modem od firmy Cisco, který je označený jako MD-1. Tento modem zároveň funguje i jako router, proto není potřeba připojovat další zařízení s funkcí routeru a zároveň s bezdrátovým přenosem dat.

Pomocí USB přístupového bodu, který je označený AP-1, je připojen do sítě stolní počítač PC-1. Implicitně není vybaven bezdrátovou síťovou kartou, a proto bylo nutné připojit a nainstalovat tento USB přístupový bod, který umožňuje bezdrátové připojení k síti.

K počítači PC-1 je připojena také multifunkční tiskárna označená LT-1. Tiskárna umožňuje krom samotného tisku i skenovat nebo kopírovat dokumenty. Jedná se o totožný model, jako který se nachází v 1. kanceláři. Snadno se tak zařízení spravují a udržují, není třeba řešit nákup různých tonerů například.

Jako další zařízení se zde vyskytuje notebook NB-1, mobilní telefon MB-1 a ostatní OZ zařízení.

2.3.1 Přehled zařízení v kanceláři 2

Druhá kancelář obsahuje značně menší množství zařízení. Tabulka s přehledem zařízení je tedy celkem neobsáhlá. Stejným postupem je provedeno označení jednotlivých zařízení. Formální zápis je ponechán.

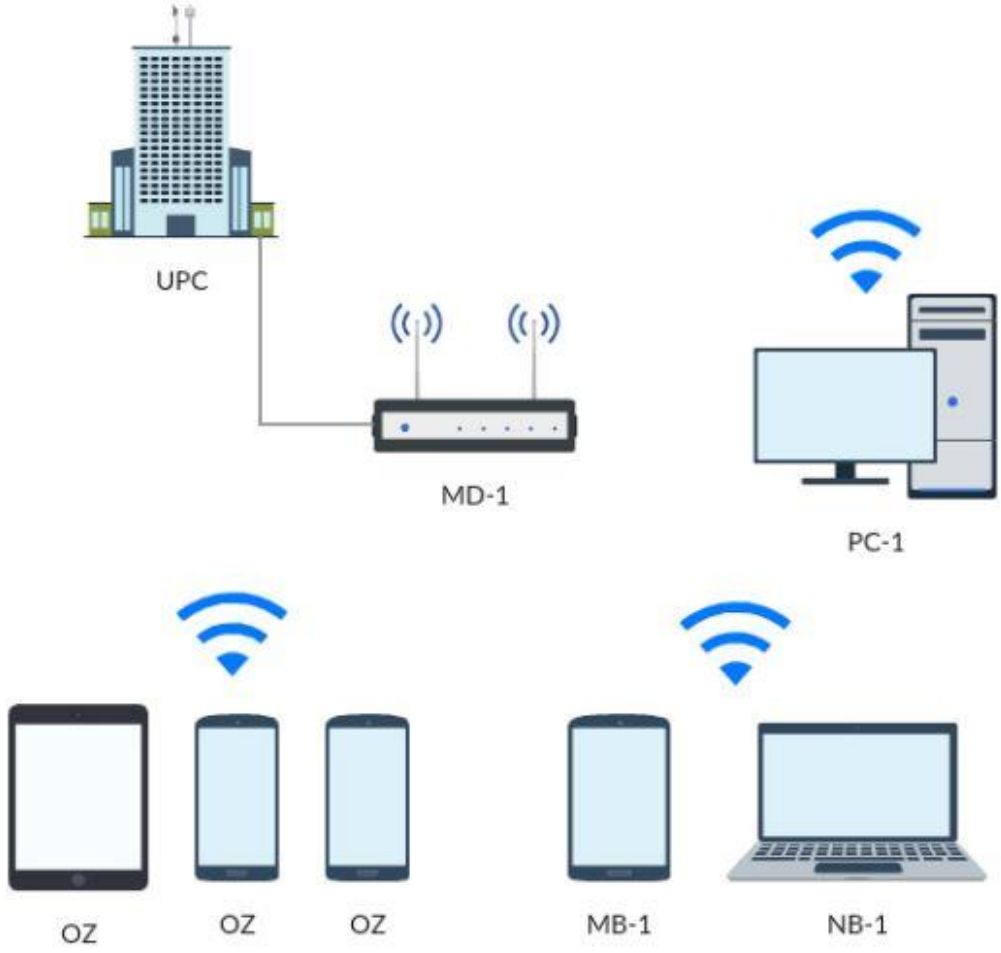
Modem, který je zároveň routerem, je označený jako MD-1, přístupový bod AP-1, stolní počítač PC-1. Dalšími síťovými zařízeními jsou laserová multifunkční tiskárna, notebook, mobilní telefon a ostatní zařízení.

Tab. 4 Přehled zařízení kancelář 2

Název zařízení	Označení	Umístění
Modem Cisco EPC3925	MD-1	CH
USB přístupový bod TL-WN722N	AP-1	OB
Stolní PC	PC-1	OB
Notebook Asus	NB-1	OB
Laser tiskárna HP LJ M1132	LT-1	OB
Mobilní telefon	MB-1	OB
Ostatní zařízení návštěvy	OZ	PZ

2.3.2 Topologie s diagramem sítě kanceláře 2

Na obrázku je možné vidět logické rozložení síťových zařízení v kanceláři 2.



Obr. 4 Topologie s diagramem sítě kanceláře 2

2.3.3 Schéma adresace v kanceláři 2

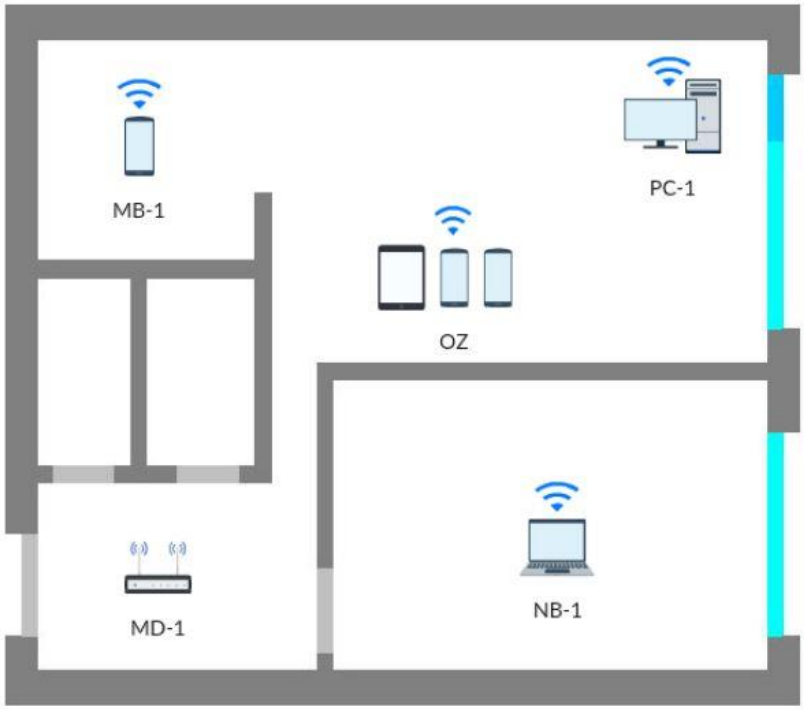
V tomto případě se IP adresy všech zařízení přiřazují pouze dynamicky pomocí DHCP serveru, který je také součástí MD-1 routeru.
Výchozí brána má také adresu 192.168.1.1 jako v kanceláři 1. A maska sítě je zde také 255.255.255.0.

Tab. 5 Schéma adresace kancelář 2

Zařízení	Přiřazení IP adresy	IP adresa	Výchozí brána	Maska sítě
MD-1	Staticky	192.168.1.1	-	255.255.255.0
PC-1	DHCP	-	192.168.1.1	255.255.255.0
NB-1	DHCP	-	192.168.1.1	255.255.255.0
MB-1	DHCP	-	192.168.1.1	255.255.255.0
OZ-1	DHCP	-	192.168.1.1	255.255.255.0

2.3.4 Grafické rozložení kanceláře 2

Grafické rozložení kanceláře můžeme vidět na následujícím obrázku, který můžeme následně porovnat s kanceláří 1. Stavebně je kancelář řešena stejně jako v první kanceláři.



Obr. 5 Grafické rozložení kanceláře 2

Výměry místností zobrazuje následující tabulka. Jedná se o kancelář 2, jejíž grafické rozdělení bylo zobrazeno na obrázku 5.

Tab. 6 Výměry místností kancelář 2

Místnost	Výměra
Kuchyň (OB)	28,00 m2
Pokoj 1 (PO)	11,78m2
Předsíň (CH)	6,80m2
Koupelna	1,65 m2
WC	0,90m2
Sklep	1,50m2
Celkem plochy	48,40m2

2.4 Celkový přehled zařízení v celé počítačové síti

Pro celkový nadhled je vytvořena tabulka zobrazující veškerá zařízení v síti. Některá se v síti vyskytují vícekrát, z toho důvodu je uveden typ zařízení a jeho počet. U ostatních zařízení nám je přesný počet neznámý, proto je sloupec „Počet“ v tomto případě ponechán prázdný.

Tab. 7 Celkový přehled zařízení v celé počítačové síti

Typ zařízení	Počet
Modem	2x
Router	1x
Pevná linka	1x
PC	2x
Notebook	3x
Mobilní telefon	3x
USB Přístupový bod	1x
USB Print server	1x
Laserová tiskárna	3x
Smart TV	1x
Čtečka elektronických knih	1x
Ostatní zařízení návštěvy	

3 Analytická část

V kapitole je rozebrána analýza současného stavu počítačové sítě. Je vycházeno z předchozí kapitoly, kde je popsána lokalita, kde se síť nachází. Jsou v ní zobrazena schémata prostorů sítě, popisy zařízení, jejich označení a adresní schéma.
Dalším obsahem kapitoly je popis a analýza současného stavu kanceláře 1 i 2, taktéž celková analýza sítě. Mimo jiné kanceláře slouží taktéž k bydlení. Nicméně jak již bylo zmíněné dříve, hlavní úlohou počítačové sítě je umožnit kvalitní poskytování služeb v oblasti účetnictví a daňové a mzdové politiky. Se vším jistě souvisí kvalitní zabezpečení sítě, která obsahuje především citlivá data klientů, jeho zaměstnancích a obchodních partnerech. Jak je řešena v současném stavu antivirová ochrana?

3.1 Antivirová ochrana AVG FREE

O zajištění ochrany před nežádoucími viry se stará software od společnosti AVG ve verzi AVG Antivirus FREE. Jedná se o verzi, která je nabízena zdarma s možností vylepšení na plnou verzi. Tato bezplatná verze nabízí kromě blokování virů také proaktivní varování před nebezpečnými odkazy. Což je také velmi důležité, protože není tak složité v době nepozornosti otevřít nežádoucí webovou stránku, která je často podsunutá hackery, aby došlo k nachytání oběti a získání citlivých údajů. Této hackerské technice, která je zde stručně popisována, se říká Phishing.[5] Jedná se o podvodnou techniku používanou ve snaze získávání citlivých údajů (jako jsou hesla, přihlašovací jména, čísla kreditních karet). Principem této techniky je věrné podání emailových zpráv, které se tváří jako zpráva od banky nebo jako velmi důležitá zpráva. Oběť je nucena kliknout na odkaz, který ji přesměruje na stránku vytvořenou útočníkem a dále je oběť vyžádána vypsat výše zmíněné citlivé údaje. Je někdy velmi těžké rozpoznat pravost zprávy a proto nám pomáhají nástroje, které to rozpoznávají za nás a pomáhají nám tak ochránit naše data, údaje a v neposlední řadě peníze, o které samozřejmě hackerům jde nejvíce. Jak je tomu ovšem s touto antivirovou ochranou ve skutečnosti?
Když začneme zapnutím počítače. Stává se velmi často, že samotné spuštění trvá dlouho a to právě proto, že se čeká na spuštění AVG programu. Občas se může uživatel setkat s hláškou: „pomalý start PC?“ Související je samozřejmě další nabízení již komerčních a placených

aplikací a produktů od firmy AVG. Nabízenou aplikací při pomalém startu počítače je AVG TuneUp. Který *„dokáže zrychlit starší počítače, vyčistit roky neodstraňované dočasné soubory, zabránit programům ve zbytečném využívání prostředků, opravit chyby, dále zajišťuje svižný chod Windows, čistí nepotřebné soubory, každé 3 dny provádí automatickou údržbu, zjišťuje výkonnostní problémy atd.“*[6] Za vším, co je na první pohled zdarma, se skrývá ať už budoucí vylákání peněz od uživatele.

Pokračujeme-li v analýze, necháme spuštěný PC s antivirovou ochranou. Jako další krok následuje aktualizace virové databáze, která velmi omezí rychlost počítače při této činnosti. Někdy ho zpomalí natolik, že uživatelé nejsou ochotni dále na vše čekat a operační systém raději restartují a při dalším spuštění raději ihned aktualizaci vypnou, protože na ni nebudou přece čekat, když potřebují pracovat. Takže se pak operační systém dostává do okamžiku, kdy je vlastně zranitelný, protože nemá načtenou aktuální virovou databázi.

3.2 Zabezpečení mobilních zařízení

Zařízení mají zabezpečenou SIM kartu a sice zadání hesla (mnohdy pouze čtyřmístného). Jedná se o tzv. PIN, který se zadává při spuštění zařízení. Na jiná přihlášení není uživatel vyzván – kromě již nainstalovaných programů, jako je email klient nebo internetové bankovnictví například, kde je to jistě žádoucí.

I mobilní zařízení ukládají citlivá data, která je nutné ochránit a zabezpečit. V tomto okamžiku nám velmi pomůže nainstalovaný antivirový program i v daném mobilním zařízení. Těchto programů je na trhu nepřeberné množství, který je ale nejlepší? Tato problematika bude popsána v další kapitole.

Antivir nás ovšem nemůže ochránit před všemi vnějšími hrozbami. Mnoho infiltrací může uživatel odstínit sám. Je důležité nesouhlasit se vším, co nám systém nabídne a uvažovat nad tím, jestli je to opravdu nezbytně nutné pro používání. Mnoho aplikací totiž žádá pro své správné fungování (i když to ve skutečnosti vůbec nepotřebují) přístup ke kontaktům uživatele nebo k úložišti dat. Uživatelé jim to poskytnou a už je mají, mají jejich kontakty a třeba i data.

Dalším pravděpodobnou skutečností je stejné heslo do všech aplikací, systémů a proto se útočník po zjištění údajů snaží ty samé informace použít i v jiných aplikacích vyžadujících přihlášení. [7]

Uživatelé dále mívají nastavené odemčení mobilu pouhým přejetím prstů po obrazovce. Pakliže jsou ovšem špatné pokusy o odemčení opakovány, telefon se zablokuje na 30 sekund a není ho tak možné používat. [8]

3.3 Zálohování dat

3.3.1 Externí disk

Data se zálohují manuálně na externí disky. Na disku jsou vždy založené konkrétní adresáře pro zálohu dat a uživatelé tak provádí tuto činnost manuálně sami. Zálohování provádí několikrát do měsíce. Již se v minulosti stalo fyzické poškození disku při náhlém výpadku proudu, po této zkušenosti je prováděna záloha již mnohem častěji, než předtím.
Externí disk je k počítači připojený přes USB kabel. V současnosti, v případě opětovného výpadku proudu, není zajištěna přepěťová ochrana a tedy ve výsledku jsou ohrožena data, protože se tímto výpadkem proudu může disk poškodit. Proto je nejlepší po dokončené záloze dat opět disk odpojit a nebo disky připojit do záložního zdroje, tzv. UPS.

3.3.2 Záložní zdroj UPS (Uninterruptible Power Supply)

Nepřetržité dodávání souvisle elektrické energie nám zajišťují zařízení, kterým se říká záložní zdroje. V současné době v naší počítačové síti taková zařízení nejsou nainstalována. Funguje to tak, že při případném výpadku dodávky energie se ozve zvukový signál upozorňující uživatele na to, aby rychle ukončil veškerou svoji rozpracovanou činnost a počítač vypnul.
V dnešní době nejsou UPS zařízení nijak nedostupné. Standardní zdroj, který je určený pro menší množství připojených zařízení, můžeme koupit od 1000 Kč výše, což není, s ohledem na dřívější ceny těchto zařízení, tak drahé. [9]
Nejdůležitějším parametrem zdrojů je jejich výkon udávaný ve wattech (W) a ve voltampérech (VA), dále jeho hmotnost, počet akumulátorů a jak dlouho vydrží při určitém zatížení. Bývá to od několika až po desítky minut s ohledem na počtu připojených zařízení.

3.4 Komunikace mezi kancelářemi

Komunikace je prováděna skrze telefonní hovory nebo elektronicky přes email. Při telefonování využívají uživatelé neomezených tarifů od poskytovatele. Kterému platí paušálně každý měsíc za aktuální období.
V případě potřeby zaslání dat, se využívá služeb emailu. Když je potřeba zalast větší soubor, uživatelé ho nahrají na cloudové úložiště Google Disk, které nabízí zdarma nahrání dat do velikost 15 GB nebo přes Dropbox úložiště, které je omezené na 2 GB (taktéž v nezpoplatněné verzi).
Mezi další možnost, jak sdílet data, je uložení dat na flash disk a následné fyzické předání. Což je využíváno hlavně při potřebě uchovat citlivá data mimo internet. Tím, že se nahrají do cloudu, jsou svým způsobem již ohrožená.

4 Zhodnocení a doporučení

V této kapitole se věnujeme doporučení, návrhu a popisu nového nabízeného řešení na realizaci počítačové sítě.

4.1 Antivirová ochrana

Aby byla síť lépe zabezpečená a aby byla zajištěna lepší odezva počítačů, byla provedena změna, která značně přispívá ke zlepšení. Antivirová ochrana AVG FREE nevyhovuje v mnoha pohledech, které byly zmíněny v předchozí kapitole a proto bylo provedeno rozhodnutí o změně.
Prvním faktorem, který zohledníme, je zátěž programu na hardware počítače. Výběrem jsou aplikace nezabírající tolik paměti RAM (operační paměť počítače) a aplikace, které nemají tak vysoké nároky na procesor při startu systému, tím pádem ho tolik nezatěžují a umožňují plynulé spuštění. Dle analýzy je tento faktor klíčový, proto byl zohledněn.

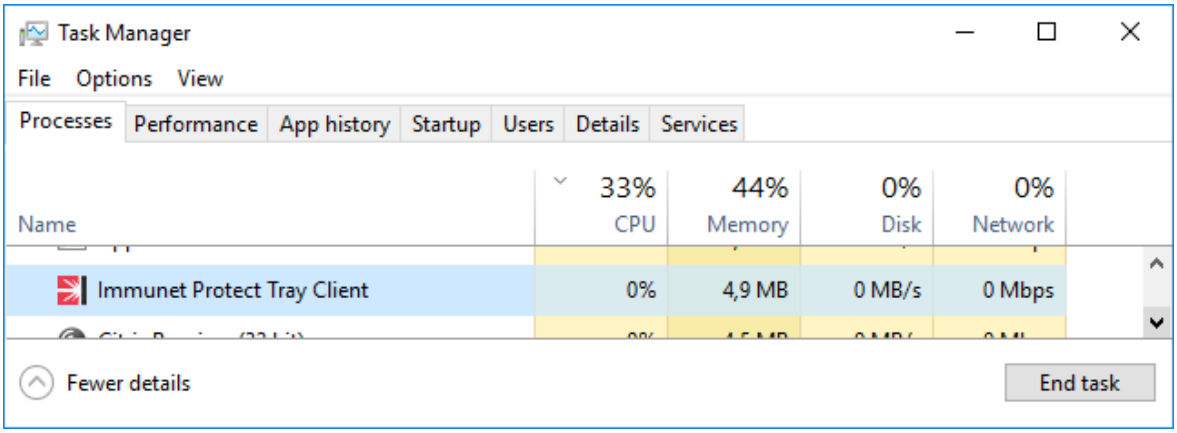
4.1.1 Cloudové řešení antiviru

Po hledání a zkoumání nejvhodnějšího typu antiviru bylo vybráno řešení tzv. „cloudových“ typů antiviru. V praxi je řeč o tom, že systém, který nás chrání před viry, neukládá do počítače

aktuální virovou databázi, ale je připojený do takové databáze online. Obrovskou výhodou je právě požadovaná náročnost aplikace na operační systém. Konvenční antivirové programy jsou pro samotný provoz aplikace výpočetně náročné a ještě náročnější při stahování aktualizací virové databáze. Tato operace zabere mnohdy i desítky minut (záleží na četnosti aktualizací) a velice omezí v danou chvíli uživateli práci, protože se v podstatě musí počkat, než se aktualizace dokončí. Cloudové antivirové systémy nabízí stálé připojení k virové databázi a proto nemusíme čekat na stahování velikých balíků dat, navíc máme databázi stále aktuální. [10]

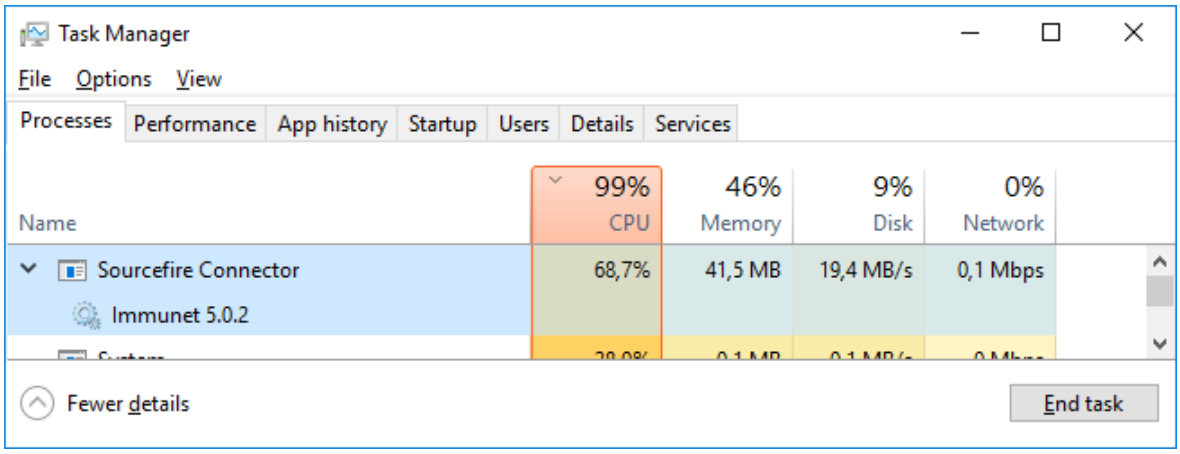
4.1.2 Immunet

Aplikace Immunet je cloudovým antivirovým systémem, který byl nainstalovaný do naší počítačové sítě. Jedná se o velice nenáročnou aplikaci na výkon počítače, nezatěžuje tolik procesor ani operační paměť RAM. Výrobce umožňuje stažení a nainstalování programu zdarma za účelem rozšíření komunity uživatelů, nenabízí nežádoucí reklamy při jeho provozu a verze není omezená. Má jednoduché grafické rozhraní a taktéž jednoduché i nastavení. Jedná se o velmi „user friendly“ (uživatelsky přívětivé) rozhraní.
Když byla provedena analýza, jak je aplikace náročná, bylo zjištěno, že si program opravdu nerezervuje tolik místa v operační paměti, při běžném provozu je spotřebováno okolo 5 MB. Náročnost aplikace je samozřejmě zvýšena při aktivním testování a při hluboké analýze.



Obr. 6 Testování TaskManager 1

Na obrázku můžeme vidět Task Manager, který zobrazuje náročnost aplikace Immunet při běžném provozu. Operační paměť je spotřebována okolo 5 MB a procesor v 0 procent. Při hluboké analýza a testování je pak procesor využit naopak téměř ze svých 100 procent.



Obr. 7 Testování TaskManager 2

4.2 Zabezpečení mobilních zařízení

V předešlé kapitole byla provedena analýza, jakým způsobem jsou zabezpečeny mobilní zařízení. Závěrem analýzy byla nutnost se více zaměřit na zabezpečení mobilních zařízení, protože stávající řešení příliš bezpečné není. Proto je navrženo nové řešení, které zamezí nepříjemným okamžikům se zabezpečením sítě.

V případě zaměření se na antivirové programy mobilních zařízení, nelze si nevšimnout společnosti Webroot, nabízející produkt SecureAnywhere® Mobile, která je určená pro zařízení se systémy iOS i Android. Tuto aplikaci využívají všechny zařízení v síti, kromě klientů a návštěv, kteří se připojí pouze dočasně v době schůzky.

Webroot aplikace je nabízena ve dvou verzích. Je možné si koupit komerční verzi Premier za necelých 15 dolarů ročně nebo je možné používat bezplatnou verzi aplikace, která je ovšem omezená, nemá veškeré nabízené funkce. I přesto jsem tuto bezplatnou verzi nainstaloval do všech mobilních zařízení v síti, protože i tato verze je po funkční stránce velmi dobrá. Srovnání je provedeno pomocí tabulky, kde je porovnána komerční i bezplatná verze aplikace.

Tab. 8 Srovnání Webroot

Funkce	Plná verze	Bezplatná verze
Antivirus	ANO	ANO
Secure Web Browsing	ANO	ANO
DeviceLocate&Scream	ANO	ANO
DeviceLock	ANO	ANO
Call & SMS Blocking	ANO	ANO
SecurityShields	ANO	ANO
Mobile SecurityWebsite	ANO	ANO
SIM CardLock	ANO	NE
DeviceWipe	ANO	NE
VulnerableSysteSettingsAlert	ANO	NE
AppInspector	ANO	NE
Battery& Network Monitor	ANO	NE

Z tabulky můžeme zpozorovat, že i v bezplatné verzi si nalezneme v podstatě vše, co je potřeba. Mezi nejdůležitější funkce zařadíme Antivirus a Secure Web Browsing zajišťující bezpečně prohlížet webové stránky. Mezi další výhody programu patří jednoduché webové rozhraní, skrze které se můžeme starat o veškerá naše zařízení, které mají samozřejmě aplikaci nainstalovanou.

V případě, že by došlo ke krádeži zařízení, jsou zde nabízené možnosti zařízení ochránit - hlavně data, která má uvnitř. Přes webovou aplikaci je možné se přihlásit a vzdáleně provést zamčení zařízení nebo napsat na obrazovku jakýkoli text. Aby bylo možné odemknout zařízení, je požadováno zadat heslo, které můžeme spravovat právě přes webové rozhraní.

Dále aplikace nabízí lokalizovat zařízení pomocí GPS signálu. Při zaměření GPS systémem na přístroji, se na mapě ve webové aplikaci zobrazí během chvilky, kde se dané zařízení nachází. Velmi záleží, jak má zařízení kvalitní GPS signál a kde se právě nachází. Není to ovšem úplně dokonalé. Při provádění testů se ne jednou zobrazila hláška, že zařízení není nalezené.

Jedinou podmínkou aby vše správně fungovalo, je připojit přístroj k internetu, protože když by připojené nebylo, není samozřejmě možné jej přes webové rozhraní nějak spravovat a tím pádem dostatečně zabezpečit. Je samozřejmostí, že ne všechna zařízení jsou stále připojená k internetu, proto je i možnost tyto vychytávky nevyužít.

V neposlední řadě je nutno zmínit ještě funkci blokování volajících a SMS od různých uložených i cizích kontaktů. Taktéž lze pomocí webového rozhraní různě upravovat seznam

těchto nežádoucích kontaktů. To bylo velmi uvítáno, protože uživatelé se stále setkávají s tzv. marketingovou masáží a pořád někdo volá s nabízením nových skvělých produktů. Tímto můžeme tyto kontakty a společnosti blokovat a zajistit si tak klid na jiné činnosti, na které se potřebujeme soustředit. [11]

4.3 Zálohování dat

Ruční kopírování není příliš efektivní a vhodné. Snadno se stane, že se zálohování provádí nahodile a také se může stát, že v případě opravdového problému nemáme potřebná data k dispozici. Hledají se zálohy, které můžou být týdny či měsíce staré a proto je nejvhodnějším řešením nastavit pravidelné zálohování, které se provádí automaticky. Zálohy tak budou stále aktuální a nemůže se stát, že by nám měsíce chyběla data. Důležité je ovšem správné nastavení.

4.3.1 EaseUS Todo Backup Free

Jedním takovým zálohovacím programem je software společnosti EaseUS a sice EaseUS Todo Backup ve verzi Free. Podmínkou pro užívání této aplikace je zaregistrování se u EaseUS. Po vykonání registrace je možné software užívat. Má velmi přívětivé a intuitivní rozhraní, instalují se pravidelné aktualizace a je zajištěna podpora dodavatele. Program je dostupný pro uživatele operačních systémů Windows, ale také MacOS. Aplikace je pouze v angličtině, což může české uživatele odradit, ale v našem případě to nevadí.

V aplikaci lze nastavit pravidelné zálohy celého OS, toto nastavení pro zkušenější uživatele je možné provést opravdu na pár kliků. Rozhodně bych pozitivně zhodnotil jednoduché ovládání a přehledné rozhraní aplikace. Samotné zálohování celého operačního systému funguje tak, že se vytvoří image (obraz) disku, který je následně v případě potřeby možný rozbalit a obnovit tak zálohovaná data.

Kromě zálohy celého operačního systému lze také nastavit zálohu vybraných adresářů. V praxi to znamená to, že si třeba vytvoříme adresář „důležité“ a na ten nastavíme zálohování. Zálohování může být provedeno na základě požadavku plánovače, který nejdříve pečlivě nastavíme a pak můžeme nechat automatické zálohování na aplikaci. Občas je ovšem dobré zkontrolovat skutečnost a jestli je vše v pořádku. O to se postará buď správce nebo uživatel sám.

Existují různé formy zálohy. Buď se dělá plná záloha nebo přírůstková, či rozdílová. Plná záloha provede zálohování všech adresářů a souborů bez ohledu na změny. Tato plná záloha je nastavena pouze jednou měsíčně, není potřeba ji provádět častěji.
Dále je nastavené také přírůstkové zálohování, které funguje tak, že se zálohují pouze změněné adresáře nebo soubory od poslední zálohy – změní-li se soubor nebo obsah adresáře. Ostatní zálohované není. Tento způsob velmi ušetří kapacitu disku, protože se nezálohují všechny soubory a adresáře, ale jen vybrané.
Rozdílové zálohování je velmi podobné tomu přírůstkovému, jen doba po kterou se obnovují data je kratší. Tuto zálohu je vhodné dělat častěji, něž zálohu plnou. Zálohovaná data jsou ukládána na externí disk, který je připojen k počítači.

4.3.2 Záložní zdroj UPS (Uninterruptible Power Supply)

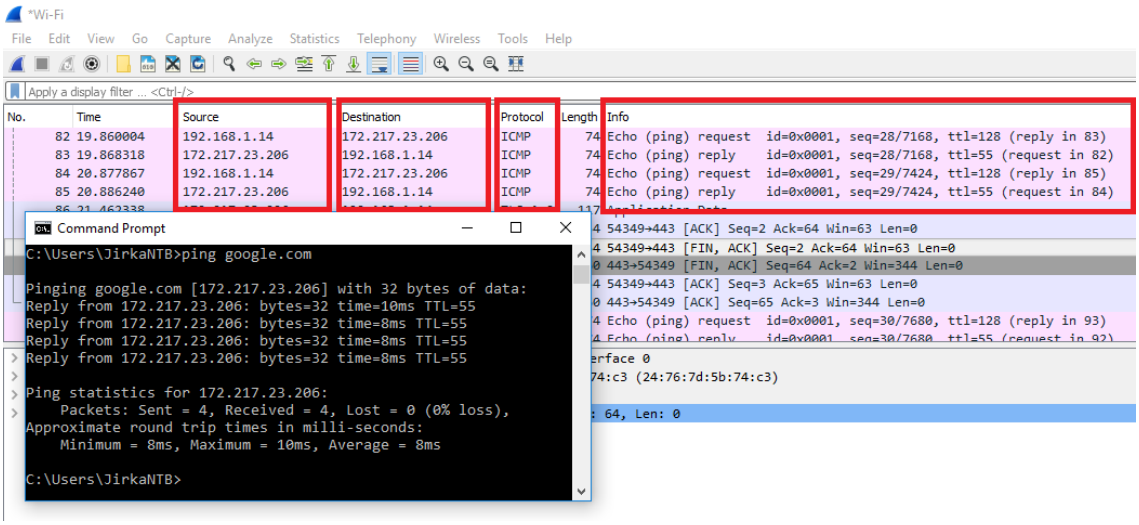
Pořízení záložního zdroje se očekává až koncem letošního roku. V současné době nouzového stavu je otázka, jak vše dopadne.

4.4 Propojení sítí přes VPN tunel

V dnešní uspěchané době je komunikace pouze přes telefon nebo e-mail velmi omezující. A proto bylo na základě analýzy vyhodnoceno optimální řešení dané problematiky a sice propojit kanceláře přes VPN síť, tzv. vytvoření VPN tunelu mezi nimi. Základní podmínkou je připojení k internetu na obou stranách tunelu. Po připojení obou kanceláří k internetu a již zajištěném nastavení lokální sítě na každé straně tunelu, je možné implementovat VPN tunel. Pro správné fungování propojení sítí, je nezbytné, aby jedna kancelář byla nastavena jako server, k němuž se připojí tzv. klient, což znamená v našem případě kancelář druhá. Jako podpůrná aplikace pro implementaci VPN tunelu byla zvolena OpenVPN aplikace, která je opět velmi jednoduchá na instalaci a konfiguraci.[12]

5 Testování

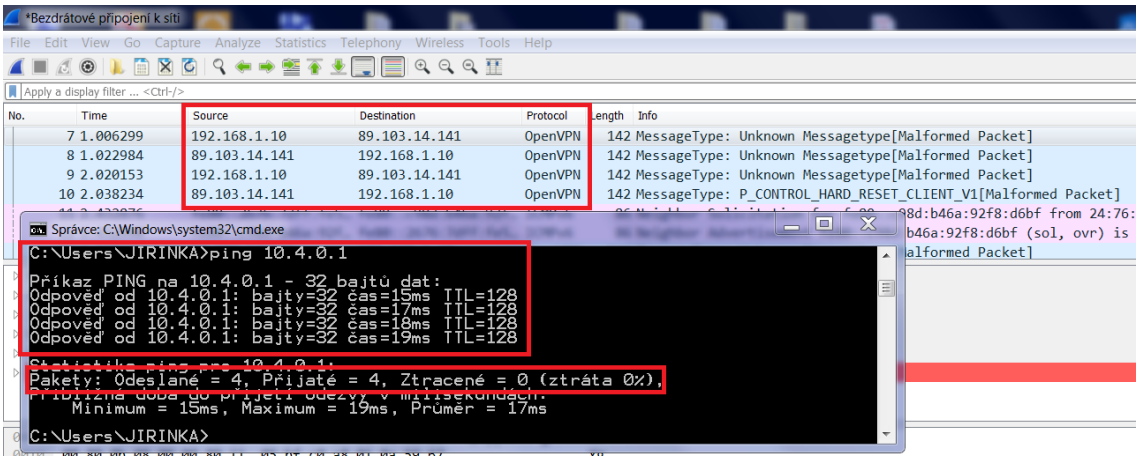
5.1 Dostupnost internetu v kanceláři



Obr. 8 Testování Wireshark

Na výše zobrazeném obrázku můžeme vidět výstup z programu Wireshark [13] a také z příkazové řádky Windows. Test byl proveden spuštěním příkazu „ping google.com“, tím jsme ověřili dostupnost internetu z kanceláře. Zdrojová IP adresa je 192.168.1.14 (přidělená pomocí DHCP). Když zapíšeme příkaz „ping“ se doménový název „google.com“ přeloží pomocí DNS záznamů na 172.217.23.206. Přes ICMP protokol (Internet Control Message Protocol) [14] se pošle request (požadavek) na ověření dostupnosti cílové adresy, za níž se schovává server, který odpovídá na požadavky. To je vidět na řádku 83 jako reply (odpověď). Zdroj a cíl se otočí a pošle se odpověď tomu, kdo se ptal. Test nám tedy odhalil, že se na server google.com můžeme připojit, protože je dostupný. Lze to vidět i v příkazovém řádku Windows, že se dostávají odpovědi od google.com – řádek „Reply from 172.217.23.206“ ve formě 32 bytových packetů. Připojení k internetu je tedy v pořádku.

5.2 Komunikace mezi kancelářemi

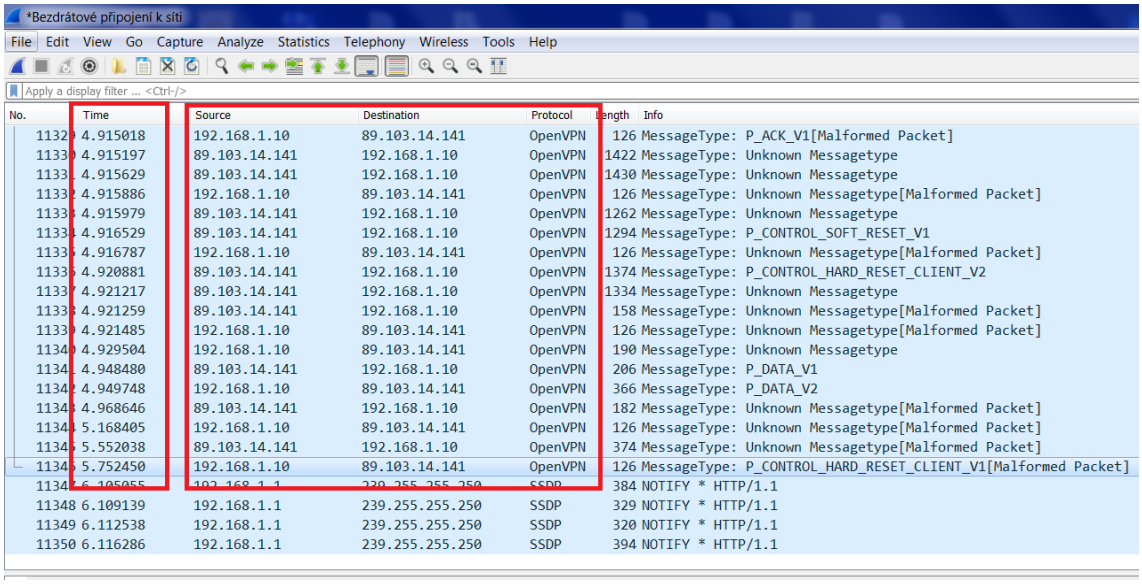


Obr. 9 Testování komunikace mezi kancelářemi

Pomocí programu Wireshark byl proveden i test komunikace mezi kancelářemi. Z příkazové řádky Windows byl zaslán ping na adresu 10.4.0.1, kterým si ověřujeme dostupnost cílového počítače (PC-1 v kanceláři 1), jestli je dostupný pro komunikaci. Lokální adresa 192.168.1.10 je zdrojovou IP adresou počítače PC-1 ve 2. kanceláři. Adresa 89.103.14.141 představuje adresu cílového serveru, který je dotázán. Pomocí routovací tabulky (směrovací tabulka) je přeložena adresa 10.4.0.1 na 89.103.14.141 – což je veřejná IP adresa první kanceláře. Kanceláře jsou spojeny pomocí OpenVPN protokolu, který umožňuje komunikaci mezi oběma kancelářemi přes aplikaci OpenVPN. Testování komunikace probíhá skvěle, ze 4 poslaných packetů máme nulovou ztrátu. Kanceláře mezi sebou tedy komunikují bez problému.

5.3 Poslání souboru mezi kancelářemi

Test byl proveden na základě poslání souboru o velikosti necelých 10 MB z druhé kanceláře do první. Na stolním počítači v první kanceláři byla vytvořena veřejná složka, do které byl soubor zaslán. Na obrázku 10 lze vidět, jak spolu komunikují klient/server, což v našem případě představují stolní počítače v obou kancelářích. Zasílají si požadavky a odpovědi, vzájemně si vyměňují packety přes protokol OpenVPN. Celý proces trvá 5,75 sekundy, takže naprosto dostačující pro nejběžnější posílání text souborů nebo PDF dokumentů. Poslání souboru netrvá tak dlouho, jako fyzické předání dat druhému uživateli na flash disku.



Obr. 10 Testování zasílání souboru

5.4 Testy rychlosti připojení k internetu

5.4.1 Kancelář 1

V níže uvedené tabulce jsou přehledně zobrazeny výsledky testování rychlosti připojení, konkrétně rychlost stahování a nahrávání. Nejlepší výsledky byly dosaženy v OB a v PO místnostech, naopak nejpomalejší rychlosti byly na NB-1 zařízení, které je přes WiFi připojené v místnosti LO.

Tab. 9 Testy rychlostí kancelář 1

Označení	Umístění	Připojení	Rychlost stahování	Rychlost nahrávání
PC-1	OB	LAN	95,16 Mbit/s	30,27 Mbit/s
NB-1 WiFi	LO	WiFi	5,08 Mbit/s	10,44 Mbit/s
NB-2	PO	LAN	94,50 Mbit/s	30,56 Mbit/s
NB-2 WiFi	PO	WiFi	14,34 Mbit/s	23,01 Mbit/s
MB-1	PO	WiFi	7,09 Mbit/s	15,00 Mbit/s
MB-1	LO	WiFi	26,12 Mbit/s	21,46 Mbit/s
MB-1	OB	WiFi	34,20 Mbit/s	30,39 Mbit/s
MB-2	OB	WiFi	34,74 Mbit/s	28,17 Mbit/s
MB-2	PO	WiFi	7,73 Mbit/s	19,99 Mbit/s
MB-2	LO	WiFi	15,47 Mbit/s	18,17 Mbit/s

5.4.2 Kancelář 2

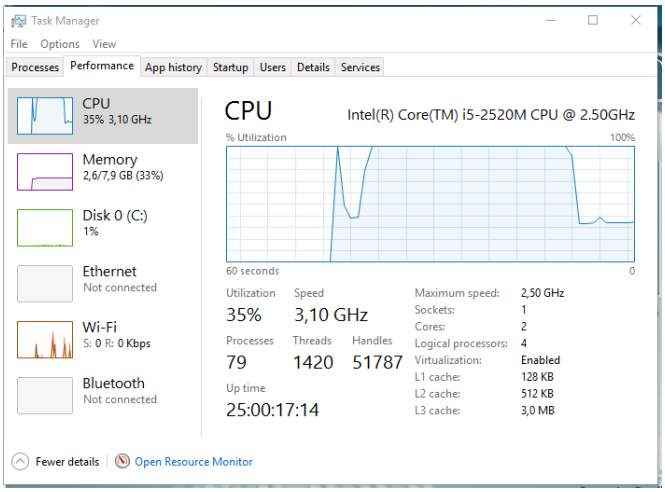
Stejný test jsme provedli v druhé kanceláři. Nejlepší rychlosti byly zaznamenány na NB-1 v místnosti OB.

Tab. 10 Testy rychlostí kancelář 2

Označení	Umístění	Připojení	Rychlost stahování	Rychlost nahrávání
PC-1	OB	WiFi	23,74 Mbit/s	20,35 Mbit/s
NB-1	OB	WiFi	56,15 Mbit/s	20,26 Mbit/s
MB-1	OB	WiFi	31,29 Mbit/s	20,30 Mbit/s
MB-1	LO	WiFi	33,65 Mbit/s	20,68 Mbit/s

5.5 Testování antiviru

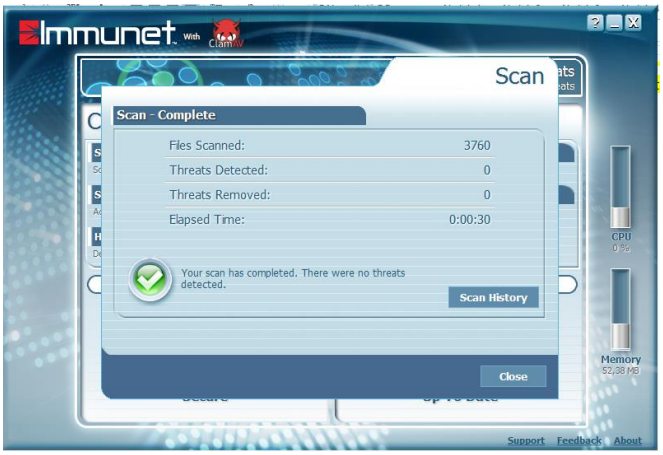
Zde je provedena analýza rychlosti antivirového testu celého počítače. Aplikace Immunet nabízí 3 možnosti testování. Rychlý sken běžících procesů, skenování konkrétních složek v počítači a test celého počítače. Rychlé oskenování běžících procesů se dokončí zhruba za půl minuty s vytížením procesoru na 100 procentech téměř po celou dobu testování.



Obr. 11 Testování antiviru 1

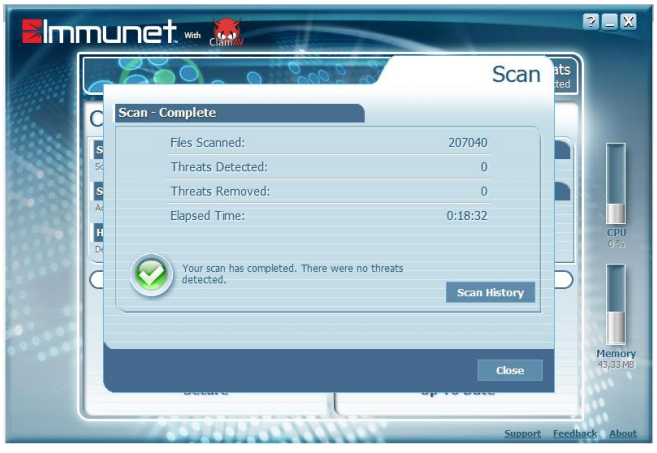
Musíme počítat s velmi vysokým vytížením procesoru při této možnosti testování běžících procesů. Na druhou stranu to netrvá tak dlouho, aby se to nedalo zvládnout, na chvíli test spustit a nechat jej pracovat. Přímo v aplikaci Immunet je pak po dokončení testu přehledně

vidět kolik bylo testovaných souborů, kolik bylo detekováno a vymazáno hrozeb a jak dlouho test trval. Tento přehled je zobrazen na následujícím obrázku.



Obr. 12 Testování antiviru 2

Pokud necháme provést hloubkovou analýzu, ta je pak časově náročnější a doba trvání se odvíjí od množství souborů a dat na disku. Čím je disk plnější a obsahuje více souborů a dat, tím test trvá déle. Tady je ovšem příjemné, že procesor není po celou dobu testování maximálně využit a jeho zátěž tedy kolísá. To znamená, že lze při této možnosti testování s počítačem normálně pracovat a uživatel je jen částečně omezen, protože část výpočetního výkonu si bere samotné testování. V našem případě tato hloubková analýza trvá okolo 18 minut.



Obr. 13 Testování antiviru 3

6 Závěr

Cílem této práce bylo vybudovat firemní počítačovou síť a propojit dvě lokální kanceláře, které spolu budou komunikovat v rámci jedné sítě. Cíle byly úspěšně dosaženy dle zadání. Velikou radost mám nejen z úspěšného dokončení stanovených cílů, ale také ze samotného psaní všech částí práce – od popisu stavu řešené problematiky, přes provádění analýzy, po zhodnocení a návrh lepšího řešení, které bylo následně důkladně otestováno.

V kapitole popisující současný stav poznání řešené problematiky, jsem se věnoval charakteristice počítačové sítě, ve které jsem popsal její umístění. Síť, která byla původně rozdělená mezi dvě kanceláře, jsem popsal podle umístění jednotlivých kanceláří zvlášť. V obou kancelářích jsem přehledně uvedl všechna zařízení, která jsou zainteresována v síti. Popsal jsem přehled adresací jednotlivých síťových zařízení, logická a fyzická schémata zapojení, jejichž celkový přehled jsem popsal v tabulce, která zobrazuje vždy typ zařízení a počet výskytů v síti.

Provedl jsem hloubkovou analýzu stavu sítě s ohledem na zabezpečení mobilních i dalších síťových zařízení a také antivirovou ochranu. Analyzoval jsem způsob zálohování dat a vzdálenou komunikaci mezi dvěma kancelářemi.

Po provedení analýzy jsem řešení zhodnotil a podal mnou doporučený návrh na řešení nové. Mé doporučení vedlo nejen ke zlepšení bezpečnosti uložených citlivých dat včetně bezpečnějších mobilních zařízení, ale také k zavedení automatického zálohování dat, které je uživatelsky velmi přívětivé a snadné na údržbu. Zajistil jsem rychlou a snadnou obnovu těchto zálohovaných dat, aby k nim bylo možné co nejrychleji přistoupit v případě jakéhokoli problému nebo nehody.

V poslední části jsem otestoval navržené řešení, které na základě výsledků testů považuji za úspěšné. V neposlední řadě vnímám úspěch i v mém osobním rozvoji tzv. těžkých i lehkých schopností. Mezi těžkou schopnost (hard skill), kterou jsem během zpracování této práce získal, řadím technickou znalost problematiky počítačových sítí. A získanými lehkými schopnostmi (soft skills) jsou určitě zodpovědnost a schopnost udržet strukturovaný přístup k psaní bakalářské práce.

Práci lze ještě rozšířit o instalaci a otestování záložních zdrojů UPS, které jsem na základě analýzy doporučil zainteresovat do počítačové sítě. Pořízení a instalace byla naplánována na 4. kvartál letošního roku z finančních důvodů. Bohužel současná doba je velice nejistá s ohledem na celosvětovou pandemickou situaci, která nejen pro uživatele (firmu), ale také pro mnoho dalších domácností způsobila neblahé finanční potíže. Kvůli tomuto problému

bylo majiteli firmy rozhodnuto posečkat s tímto finančním krokem, ale zároveň se s ním počítá. Uživatelé a zároveň majitelé počítačové sítě chtějí pořídit výkonnější záložní zdroje a zainvestovat tak větší peníze do těchto zařízení to a v obou kancelářích, ale v současné nejisté době se jedná o lehce riskantní krok. Proto bylo pouze podáno doporučení, které bylo následně majiteli schváleno do rozpočtu na poslední 3 měsíce letošního roku. Jsem velice rád, že mé řešení bylo schváleno v dohledné době. Ostatní změny, které jsem realizoval, byly s velkým potěšením přijaty všemi uživateli sítě. Nejvíce hrdý jsem na změnu, v rámci které se mi podařilo přes VPN tunel propojit obě kanceláře do jedné společné počítačové sítě, skrze kterou lze nejen posílat běžné soubory, ale také bylo umožněno používat aplikace komunikující právě přes jednu lokální síť s využitím klient-server síťové architektury.

7 Seznam použitých zdrojů

[1] JOBS, S. Citáty slavných osobností. *Steve Jobs citáty* [online].2020 [cit. 2020-09-20]. Dostupné z WWW:<https://citaty.net/autori/steve-jobs>

[2] Oficiální stránky společnosti UPC, [online]. Praha : UPC 2020 [cit. 2020-09-21]. Dostupné z WWW: <https://www.upc.cz/internet/nabidka/porovnani>

[3] Oficiální stránky aplikace Creately, [online]. Praha : Creately 2020 [cit. 2020-09-21]. Dostupné z WWW: <https://creately.com/app>

[4] WITZANY, J.; VRBA, J.; HONZÍK, V. Otvory v panelových domech. 1. vydání, Informační centrum ČKAIT s.r.o., 2014. 132 s. ISBN 978-80-87438-55-8

[5] Oficiální stránky společnosti Bezpečný internet.cz, [online]. Praha : Phishing 2020 [cit. 2020-10-01]. Dostupné z WWW: <http://www.bezpecnyinternet.cz/zacatecnik/e-mail/phishing.aspx>

[6] Oficiální stránky společnosti AVG, [online]. Praha : AVG 2020 [cit. 2020-10-01]. Dostupné z WWW: <avg.com>

[7] KILIÁN, K. Svět androida. *Pět zásadních kroků, jak ochránit svého androida před viry* [online]. 2015-02-11 [cit. 2020-10-02]. Dostupné z WWW: <https://www.svetandroida.cz/android-viry-ochrana-201502>

[8] ELENKOV, N. *Android securityinternals*. 1. vydání, San Francisco : NoStarchPress, Inc., 2015. 407 s. ISBN 978-1-59327-581-5.

[9] Oficiální stránky společnosti Alza.cz, [online]. Praha : Alza.cz 2020 [cit. 2020-10-12]. Dostupné z WWW: <alza.cz>

[10] KILIÁN, K. Cnews.cz. *Immunet: Jak nenáročný cloudový antivir obstál v porovnáním s Pandou* [online]. 2013-09-27 [cit. 2020-10-20]. Dostupné z WWW: <https://www.cnews.cz/clanky/immunet-jak-nenarocny-cloudovy-antivir-obstal-v-porovnani-s-pandou>

[11] Oficiální stránky společnosti Webroot, [online]. USA : Webroot 2020 [cit. 2020-11-03]. Dostupné z WWW: <https://www.webroot.com>

[12] Oficiální stránky OpenVPN Technologies, Inc [online]. USA : OpenVPN Technologies, Inc 2016 [cit. 2020-11-24]. Dostupné z WWW: <https://openvpn.net>

[13] Oficiální stránky aplikace Wireshark [online]. USA : Wireshark 2021 [cit. 2021-01-14]. Dostupné z WWW: < https://www.wireshark.org>

[14] Oficiální stránky společnosti Network Sorcery, Inc. [online]. USA : ICMP 2021 [cit. 2021-02-12]. Dostupné z WWW: <http://www.networksorcery.com/enp/protocol>