

Univerzita Hradec Králové
Fakulta Informatiky a Managementu
KIT – Katedra informačních technologií

Koncept Moderní IT infrastruktury firmy střední velikosti

Bakalářská práce

Autor: Jan Jušta

Studijní obor: Informační Management

Vedoucí práce: Ing. Pavel Blažek, Ph.D.

Hradec Králové

Srpen 2022

Prohlášení:

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a uvedl jsem všechny použité prameny a literaturu.

V Hradci Králové dne 15.8.2022



Jan Jušta

Poděkování:

Děkuji Ing. Pavlu Blažkovi, Ph.D. za odborné vedení práce, poskytování rad a zájem o úspěšné dokončení.

Taktéž bych rád věnoval poděkování Martinu Tučkovi, IT specialistovi firmy PATRON-IT, který mi byl nápomocen v rámci konzultací při závěrečné korekci bakalářské práce.

Anotace

Předmětem bakalářské práce je sběr, porovnání a návrh implementace znalostí o nových technologiích, jako je virtualizace, cloudové služby a kompletní síťové řešení, do prostředí středně velké společnosti. Implementační část je založena na case study nově založené pobočky mezinárodní společnosti. Ideální infrastruktury je dosaženo kombinací vhodného HW a SW řešení.

Annotation

Title: Concept of a modern IT infrastructure for a medium-sized company

The subject of the bachelor thesis is to collect, compare and propose the implementation of knowledge about new technologies such as virtualization, cloud services and complete network solutions in the environment of a medium-sized company. The implementation part is based on a case study of a newly established branch of an international company. The ideal infrastructure is achieved by a combination of appropriate HW and SW solutions.

Obsah

1 Úvod	1
2 Cíl práce	3
3 Metodika zpracování	4
4 Úvod do problematiky návrhu IT infrastruktury a cloud computingu	5
4.1 Normy a standardy.....	6
4.1.1 ITIL.....	7
4.1.2 ISO IEC IS 11801	8
4.1.3 Normy ČSN.....	8
4.2 Bezpečnost	9
4.3 Sít'	11
5 Microsoft 365 + Azure	13
5.1 Tenant	14
5.2 Azure Active Directory	15
5.3 Exchange Online.....	15
5.4 SharePoint	17
5.4.1 OneDrive	17
5.5 Teams	18
6 Sít'ová infrastruktura	18
6.1 Virtualizace	19
6.2 Poskytovatel internetových služeb.....	19
6.3 Aktivní sít'ové prvky	20
6.3.1 Router a Firewall	20
6.3.2 Switch.....	23
6.3.3 Access Point.....	23
6.3.4 Kamerový systém	23
6.3.5 Software Defined Network Controller	24
6.3.6 Network Attached Storage (NAS)	26
6.4 Pasivní sít'ové prvky	27

6.4.1 Rack	27
6.4.2 Strukturovaná kabeláž	28
6.5 Firmy a technologie síťových prvků	29
6.5.1 Cisco Systems	29
6.5.2 Ubiquiti Networks	29
6.5.3 Aruba	30
6.5.4 FortiNet	30
6.5.5 MikroTik	31
6.5.6 Intrusion Detection System/Intrusion Prevention Systém (IDS/IPS).....	31
6.5.7 Deep Packet Inspection (DPI)	31
6.5.8 Controller	32
6.5.9 Threat Management	33
7 Hardwarové vybavení firmy	34
7.1 Notebooky	34
7.2 Workstation	35
7.3 Monitory, projektory	35
7.4 Tiskárny a zobrazovací zařízení.....	36
7.5 Periferie	36
7.6 Nábytek.....	37
7.7 Konferenční místnosti.....	37
8 Softwarové vybavení firmy	38
8.1 Office 365 -> Microsoft 365	39
8.2 Adobe.....	40
8.3 Zálohy	42
8.4 Operační systémy (OS)	43
8.5 Licenční politika	44
8.6 Podnikový informační systém	44
9 Koncept vlastní implementace.....	46
9.1 Výsledky dotazníku	47

9.2 Vlastní návrh řešení.....	51
9.2.1 Analýza požadavků a potřeb firmy.....	51
9.2.2 Porovnání a výběr síťových prvků Cisco Meraki vs. UniFi Networks.....	53
9.2.3 Porovnání a výběr řešení On-premise vs. Cloud	54
9.2.4 Výběr vhodných prostorů	55
9.2.5 Návrh topologie a umístění síťových prvků na pobočce.....	56
9.2.6 Pořízení a výběr hardwaru	61
9.2.7 Výbava kanceláří a konferenčních místností.....	62
9.2.8 Výběr softwarové vybavení.....	63
9.3 Cenová kalkulace	64
10 Shrnutí.....	66
11 Závěr	68
12 Seznam použité literatury	69
13 Seznam použitých zkratk.....	76

Seznam obrázků

Obrázek 1 Exchange Online.....	16
Obrázek 2 OSI model.....	21
Obrázek 3 Disková pole RAID.....	27
Obrázek 4 UniFi DPI.....	32
Obrázek 5 Topologie sítě UniFi.....	32
Obrázek 6 Threat Management.....	33
Obrázek 7 Veeam Platform.....	42
Obrázek 8 Výsledky dotazníku.....	47
Obrázek 9 Výsledky dotazníku.....	48
Obrázek 10 Výsledky dotazníku.....	48
Obrázek 11 Výsledky dotazníku.....	49
Obrázek 12 Výsledky dotazníku.....	49
Obrázek 13 Výsledky dotazníku.....	50
Obrázek 14 Výsledky dotazníku.....	51
Obrázek 15 Porovnání On Premise vs. Cloud.....	55
Obrázek 16 Heat mapa přízemí.....	57
Obrázek 17 Heat mapa prvního patra.....	58
Obrázek 18 Topologie sítě pobočky.....	59

Seznam tabulek

Tabulka 1 Cenová kalkulace vstupních nákladů.....	64
Tabulka 2 Cenová kalkulace měsíčních plateb.....	66

1 Úvod

Koncept moderního IT řešení pro středně velkou firmu by měl být velice jednoduchý pro správu a údržbu, rozšiřitelný o potřebné fyzické moduly, a především funkční a stabilní.

Pod pojmem moderní se skrývá řešení, které je hodně pokročilé v rámci posledních trendů a zároveň dosti konzervativní v rámci prověřené a odzkoušené metodiky.

Pod pojmem moderní koncepce se taky dá představit určité systematické uspořádání jak na fyzické, tak softwarové vrstvě. Fyzické za pomoci kvalitního racku, strukturované kabeláže, popisu tras, designového zalištování a samozřejmě vhodného výběru fyzických prvků.

Softwarová vrstva obsahující programy, které vzájemně komunikují, jsou provázané a fungují výborně jako celek. IT administrátor se za jednoduchého přístupu pomocí hlavního rozhraní připojí k jednomu správcovskému účtu, z kterého řídí celkovou infrastrukturu. Také si lze představit řízenou automatizaci většiny procesů, které nemusí ručně nastavovat správce, ale stačí autorizovaný přístup a přenastavení důležitých parametrů proběhne pomocí hlasového rozhraní. Pod pojmem automatizace si lze představit mnoho možností, kterými IT technologie disponují. Docházkové systémy za pomoci hlasové, vizuální, či DNA autorizace povolí přístup, zaznamenají čas, data, fotografie, video, hlas a vyhodnotí tak správné kroky. V rámci automatizace jde především o úsporu času, který mohou klíčové osoby využít pro přínosnější záležitosti, než jsou IT procesy, jež pro mnohé „nějak běží“. Hlavním cílem každé firmy je zisk a díky zjednodušeným procesům v oblasti IT jej lze generovat s vyšší efektivitou.

Cloudová řešení jsou aktuálně největším trendem, možná spíše již standardem doby. Bezpečnost byla vždy největší slabinou lokálních datových center. Přesunem do cloudu (sdílené datové úložiště) se bezpečnost výrazně navýšila a k datům nelze tak jednoduše fyzicky přistoupit. V dnešní době už bez informačních technologií fungovat nelze. Doba se posouvá stále kupředu a v odvětví IT několikanásobně rychleji. Dnes se jedno konkrétní řešení může zdát

jako ideální, ale za pár měsíců až roků bude třeba se opět přizpůsobit době a stávající řešení rozšířit. Díky flexibilnímu návrhu nebude třeba nakupovat nový klíčový HW (Hardware), ale pouze stávající škálovat. Koncept (soupis a kombinace navržených řešení) bude v rámci implementace modelován pro nově zavedenou pobočku investiční společnosti v Hradci Králové, kde je IT řešeno více než ve standardní firmě, kde se na IT nahlíží pouze v rámci základních potřeb.

2 Cíl práce

Hlavním cílem teoretické části této práce je popsat postup tvorby konceptu a seznámit se moderními technologiemi v oblasti IT. Pro volbu optimální varianty bude třeba porovnat určité hardwarové a softwarové produkty, které jsou dnes na trhu nabízeny. K tomuto porovnání dojde v obsahu textu teoretické části. K dosažení cíle teoretické části bude využito stručných popisů technologií, produktů a služeb, aby byla zachována přehlednost. Tato část může být chápána jako základní zdroj informací, pro který lze, v případě zájmu, najít detailnější popis na internetu.

Cíl praktické části, který by měl být naplněn, je funkční a stabilní projekt nové IT infrastruktury, kterou lze spravovat z jednoho místa, včetně komplexního vybavení pobočky (nábytek, periferie atd.) s náhledem na management a lidské zdroje.

3 Metodika zpracování

Koncept (zmiňovaná case study) je zde definován jako soubor všech opatření, která budou novou pobočku provázet nejen ve vztahu k IT. Potřebné informace v praktické části bakalářské práce budou použity z již existující firmy, kde toto řešení již 5 let funguje. Modelováním rozmístění HW na pobočce se následná implementace konkretizuje. Praktická část bude obsahovat kalkulaci implementace celého konceptu, která bude vypočítána dle zvolených produktů a služeb. Kalkulace bude ovlivněná majitelem podniku a jeho chutí investovat, nicméně prioritou v implementační části bude zpracování kompletního řešení v poměru cena/výkon, aby byla udržena rozumná bilance a nebude se přeplácat za nepotřebné věci.

Pro pomoc při rozhodování o výběru nových technologií bude vytvořen dotazník, který bude zjišťovat informační vzdělanost veřejnosti v oblasti softwaru a fyzických síťových řešení. Dotazník bude rozeslán mezi osoby pracující v oboru a studenty středních a vysokých škol. Z dotazníku bude vyvozen jednoduchý a přehledný závěr, který by měl vykazovat oblíbenost daných technologií a jejich preferenci v praxi. V dotazníku budou zmíněny aktuální trendy i léta prověřené produkty. Dále bude provedená analýza potřeb konkrétního podniku a dle ní popis implementovaného řešení.

Jedním z hlavních pilířů (cílů) při implementaci síťových technologií je požadavek na zajištění vzdálené správy a dostupnosti. Díky centralizované správě by mělo být možné obsloužit více zařízení, na více pobočkách, bez toho, aby bylo potřeba využití veřejné IP adresy.

4 Úvod do problematiky návrhu IT infrastruktury a cloud computingu

Problematika návrhu IT infrastruktury je velice individuální téma, které s sebou nese mnoho času pro provedení potřebné analýzy a následné implementace včetně testování, zdali infrastruktura obstává i po několika měsících/letech při variabilním zatížení. Pro nezkušeného člověka zabere především mnoho času potřebné studium k tomu, aby se mohl racionálně rozhodnout, kterým směrem se vydá. Je třeba čerpat z mnoha zdrojů od základních norem, přes odborné publikace až po nejaktuálnější magazíny a články, které odkazují na téma oboru IT. Pro vytvoření své vlastní infrastruktury je třeba mít aspoň minimální zkušenosti s IT, ideálně praktické zkušenosti nasbírané z projektů, které byly implementovány na cizím podniku/firmě.

Prvně je nutné zjistit, jakou situaci je třeba řešit. Má se jednat o zavedení nové pobočky, rozšíření o další pobočku? Mělo by jít o úplně novou firmu? Jaké jsou její požadavky na rychlost, bezpečnost a další? Infrastruktura by měla zahrnovat veškeré produkty a služby, které se pojí dohromady. Měla by dávat ucelený provázaný systém pro reálné použití.

IT je pro většinu podnikatelů téma, kterému nerozumí a nechtějí mu věnovat více času, než je nutně potřeba, pomineme-li majitele firmy, který podniká v IT oboru. IT se většinou dává do rukou profesionálů, pro které to je denní rutina. Mají už zkušenosti i aktuální informace z oboru a díky jejich znalostem lze věci uskutečňovat rychleji a efektivněji. Je tak lepší nechat celý koncept odborníkům a jen na procesu implementace spolupracovat, aktivně komunikovat a definovat své požadavky.

Problém většiny IT odborníků je, že neumí komunikovat se zákazníkem. Umí perfektně spravovat síť, konfigurovat všechny dostupné prvky na trhu, programovat nové aplikace, ale komunikace na úrovni běžného uživatele je pro ně obtížná. Proto vždy nejvíce ceněný technik není ten, který umí udělat veškeré úkony spojené s IT, ale ten, který toto umí spojit efektivní srozumitelnou komunikací s laíkem.

Spousta firem si pro komunikaci musí najímat dalšího člověka, který funguje jako prostředník mezi zákazníkem a technikem, což je pro ně další položka v nákladech.

Pomocí cloud computingu si firma pronajímá zdroje, aplikace a služby a využívá je efektivně podle svých vlastních potřeb. Může mít přidělený a rezervovaný výkon, který skutečně využije a za něj platí měsíční poplatek. Jedná se o opačný přístup než lokálně instalovaný software. Firma využitím cloud computingu šetří místo v budově, jelikož nemá mnoho vlastních fyzických serverů, šetří finance na nákup a obnovu hardwaru i softwaru. Všechny služby a produkty jsou využívány pouze skrze internetové připojení.

Cloud computing představuje 3 hlavní modely, konkrétně SaaS, PaaS a IaaS. Software as a Service (SaaS) je služba, která poskytuje aplikace koncovým zákazníkům skrze webové rozhraní. Jedná se o obdobu lokálně instalovaných aplikací, pouze jsou užívané v cloudu. Tento model je uživateli využíván nejvíce.

Platform as a service (PaaS) je prostředí, kde se mohou uživatelé podílet na tvorbě aplikací a přizpůsobovat je svým potřebám. Je určené pro developery a vývojáře. Díky PaaS lze rychleji vytvářet nové inovativní aplikace. Vývojáři se mohou podílet nejen na psaní, ale i testování kódu.

Infrastructure as a service (IaaS) je model, který je nejčastěji užíván pro cloudovou virtualizaci. Zde si firma pronajímá pouze výpočetní výkon (zdroje). Je velice rozšířitelný a cenově dostupný. Využívá se pro běh náročných aplikací, uchovávání dat a spouštění analýz náročných na výkon. [1]

4.1 Normy a standardy

Normy a standardy užívané ve světě IT se kategorizují na mezinárodní, evropské a v případě České republiky české, které mohou být součástí těch evropských. Jedná se o souhrn technických norem, které předurčují a popisují postup návrhu, realizace, zpětné kontroly s ohledem na funkčnost, bezpečnost a jednoduchost implementovaného řešení.

4.1.1 ITIL

ITIL neboli Information Technology Infrastructure Library je mezinárodně uznávaný standard, který se využívá pro popis technologií používaných v oboru informačních technologií. Tento standard je popisován od roku 1985. ITIL se postupně rozvíjel a aktualizoval o nové verze, kdy při psaní této práce je nejaktuálnější ITIL 4, který splňuje přísné požadavky na bezpečnost a moderní technologie, je více přehledný a rozšířený o nové praktiky. Účelem tohoto standardu je popisovat nejlepší praktiky (best practices), jak řídit a spravovat IT služby ve středně velké firmě. Je vhodný pro nové podniky před jejím zavedením i pro již stávající. Poskytuje rady, tipy, varování, na co si dát pozor a propojuje business mezi zákazníkem a poskytovatelem IT služby. Dbá na spokojeného zákazníka, který využívá IT služby a poskytovatel služby na tom vydělává peníze. Pomocí ITIL lze uspořít finance i čas, jelikož není třeba vymýšlet něco nového. Profi pracovníci mají možnost získat certifikaci ITIL a stát se uznávaným pracovníkem v oboru. ITIL není chápán jako dogma, které je nutné dodržet, ale kterým by se měl nechat procesní manažer vést a přizpůsobovat si jej svým vlastním potřebám. Je skládán z vícero částí, které vedou k uspokojení obou stran – zákazníka i dodavatele.

- **Procesní řízení** – proces je jednoznačně specifikovaný a strukturovaný, flexibilní a individuálně nastavený pro každého zákazníka.
- **Zákaznický orientovaný přístup** – hledání nejlepšího řešení pro zákazníka vzhledem k jeho potřebám a požadavkům.
- **Jednoznačná terminologie** – přesný popis bez komunikačního šumu, využívání konkrétních termínů ke specifikaci požadavků, vedoucí k porozumění a následně k rychlé a kvalitně uskutečněné zakázce.
- **Nezávislost na platformě** – možná implementace v rámci vícero oborů.
- **Volná dostupnost** – rozšíření po celém světě, dostupné pro kohokoliv.

V souvislosti s využitím normy ITIL se zohledňuje především orientace na zákazníka a přesná specifikace jeho požadavků a potřeb. Se zákazníkem by se měla provést detailní analýza, ze které vyplyne řešení, které bude ideálně odpovídat ceně, výkonu a očekávání zákazníka. [2, 3]

ITIL popisuje procesy, funkce, role a celý životní cyklus služby. Není nutné využívat ITIL jako celek, nýbrž vzít si z něj přesně to, co je aktuálně potřeba.

4.1.2 ISO IEC IS 11801

ISO neboli International Organization of Standardization je mezinárodně uznávaná společnost, která se věnuje vytváření norem a standardů. Pro účely této práce je vhodné zmínit normu ISO IEC IS 11801, která se věnuje tématu strukturované kabeláže, topologii počítačových sítí a je k dispozici od roku 1995. Od tohoto roku prošla značnou aktualizací a rozšířením o nové informace např. implementace IoT (Internet of Things), inteligentní řízení či bezdrátová komunikace.

4.1.3 Normy ČSN

Normy ČSN EN jsou české technické normy, které popisují, jak by se měly určité prvky implementovat. Normy se dále číslují na jednotlivé podkategorie a vydávají v nových edicích (aktualizacích). Každá aktualizovaná verze nahradí tu předchozí. Normy vysvětlují a dávají řád, specifikují požadavky, které by měli být při realizaci dodrženy a také dohlíží na provoz a po realizační údržbu. Jedná se o parametry jako maximální horizontální délka linky, kanálu a další. Níže jsou zmíněné podkategorie normy ČSN EN 50173 pro univerzální kabelážní systémy, které jsou nedílnou součástí při přípravě na instalaci strukturované kabeláže a normy ČSN EN 50174, která popisuje plánování a instalaci kabelových rozvodů.

ČSN EN 50173-1 – popisuje všeobecné podmínky

ČSN EN 50173-2 – popisuje kancelářské prostory

ČSN EN 50173-3 – popisuje průmyslové prostory

ČSN EN 50173-4 – popisuje obytné prostory

ČSN EN 50173-5 – popisuje datová centra

ČSN EN 50173-5 – popisuje distribuované služby v budovách

ČSN EN 50174-1 – popisuje specifikace a zabezpečení kvality

ČSN EN 50174-2 – popisuje plánování a postupy instalace v budovách

ČSN EN 50174-3 – popisuje projektovou přípravu a výstavbu budov

Existuje mnoho dalších norem, které zohledňují stínění, rušení, uzemňování. Prostředí středně velké firmy odpovídá normě ČSN EN 50173-1, ČSN EN 50173-2 a normě ČSN EN 50171-1, ČSN EN 50171-2.

Normy nám dále specifikují kategorie kabelů podle jejich vlastností (především definují maximální přenosovou rychlost). Od nejlevnější a nejstarší kategorie 1 (Cat. 1) používanou pro telefonní komunikaci, zvládající přenosovou rychlost 1Mbit/s až po kategorii 8 (Cat. 8), která zvládne přenosovou rychlost 40 Gbit/s a je využívána pro páteřní spoje. Vrcholem je vysokorychlostní optická kabeláž. [4]

4.2 Bezpečnost

V souvislosti s problematikou cloudu je třeba probrat bezpečnost. Bezpečnost dat může být ohrožena při špatné konfiguraci, špatně nastavených práv pro čtení dokumentů a jejich sdílení na síti. Velkým bezpečnostním rizikem mohou být samotní interní uživatelé. Zaměstnanci či partneři, kteří mají přístup k interním dokumentům firmy a mohou je snadno zneužít i přes smluvní ujednání. Může být zneužito firemní know-how, či jiné konkurenční výhody, které firma vlastní. Data posílaná skrze internet mohou být také odposlouchávána. Jak se připravit a zajistit maximální bezpečnost? Primárně by se mělo dbát na prevenci. IT správce by měl zajistit pevně stanovené procesy, které povedou k náročnosti tvorby hesla (např. vícefázová ověření), aby zaměstnanec neměl možnost udělat chybu. Pro tyto účely je možné zmínit software Microsoft Intune, který umí ohlídat přístupy a zásady zabezpečení. Sekundárně by se mělo dbát na pravidelné vzdělávání zaměstnanců v oblasti internetových útoků, jak jim předcházet a jak se jim bránit. Také by se měla pravidelně hlídat fluktuace zaměstnanců pro zamezení úniku dat, či neoprávněného přístupu z nedbalosti.

Data mohou být také zneužita cíleným zašifrováním a požadováním finančního úplatku za přístupový kód k jejich odšifrování. Pro záchranu dat lze zajistit jejich duplicitu a redundanci. Mít data zálohovaná na více místech a možnost k nim přistupovat na více úrovních. K důležitým informacím by měl být přístup pouze na základě víceúrovňového přístupu pomocí identit a odlišení přístupových práv. Zároveň by se měly veškeré kroky automaticky ukládat, celý

systém pravidelně zálohovat, aby bylo možné se pomocí verzování vrátit k předchozím zálohám a zvrátit nechtěný útok. Neomezený přístup k celé infrastruktuře by měl být redukován na minimum lidí pro zajištění další bezpečnosti. I tak je vhodné, aby neexistoval účet, ze kterého je možné udělat úplně všechny kroky. Je vhodné mít účty oddělené s různými přístupy tak, aby pro nezvratné kroky bylo nutné udělat další kroky z jiných účtů, kdyby se k tomu hlavnímu administrátorskému přístupu kdokoli dostal. Je dobré pravidelně provádět aktualizaci přístupů, které nejsou používány či potřebné odstraňovat. Je třeba dávat pozor na nezabezpečené přístupy k datům a užívání zabezpečených protokolů.

Častou hrozbou může být nezkušenost IT administrátora s daným systémem. Nezkušený IT správce zajistí základní nastavení a vše funguje, ale nevěnuje se dostatečně bezpečnosti a rozšiřujícímu nastavení, jelikož s tím nemá zkušenosti a nechce se v problematice více vzdělávat, dokud vše funguje a nenastane nějaký problém s bezpečností. Důležitým aspektem je nenechávat výchozí nastavení a výchozí hesla k administraci. Bezpečnost ve firmě by se měla stále monitorovat a každý jednotlivý přístup by měl být zaznamenáván. Každý přístup k systému, či dílčí aplikaci by také měl být při každém přihlášení autentizován (vícefázové ověření, otisk prstu, sken sítnice, ověřování bez hesla (passwordless) pomocí tokenu, čipu či jiné externí zařízení, které povolí přístup). [5]

O bezpečnost firemních počítačů a serverů by se měl postarat profesionální antivirový software jako třeba ESET, Bitdefender, Norton, McAfee, Kaspersky, Avira a další. Antivirový software umí detekovat virus, zamezit jeho šíření a kompletně jej ze systému odstranit. Dnešní antiviry již umí monitorovat činnost při návštěvě webových stránek, komunikovat s mikrofonom a kamerou v chráněném zařízení a detekovat tím zloděje při krádeži zařízení (typicky notebooku, telefonu, tabletu). Správný antivir pro firemní použití má své vlastní ochranné mechanismy, aby nebylo možné jej jednoduše vypnout či odinstalovat.

Pokud chce mít IT správce plnou kontrolu nad bezpečností, měl by využívat nějaký způsob monitoringu. Systém, který mu automaticky hlásí veškeré změny a nemůže se tak stát, že na chybu narazí náhodou. Primárně, aby měl přehled, že veškerý software je plně aktualizovaný a že jsou aplikovaná všechna bezpečnostní

opatření ze serveru na počítače. Měla by být možnost sledovat, v jakém stavu se aktuálně nachází fyzické prvky infrastruktury. Zdali na pevném disku ještě zbývá dostatek místa, v jaké kondici se nachází atd. Monitoring IT správci umožňuje dozvědět se o možném problému dříve, než reálně nastane a ohrozí infrastrukturu.

Kromě softwarové bezpečnosti by se měl klást velký důraz i na tu fyzickou. Firma by měla být vybavená kamerovým systémem s neustálým záznamem, který je možné dohledat několik měsíců zpětně. Do klíčových místností by měl být zamezen volný přístup a aplikovaná bezpečnostní opatření jako koule na dveřích, bezpečnostní dveře ze silného materiálu znemožňující snadné zničení a přístupový systém, který jasně identifikuje přístup patřičné osoby. Fyzická bezpečnost souvisí i s provozem technické místnosti, měla by zde být zajištěna provozní teplota pro všechny hardwarové prvky pomocí klimatizace, či vzduchotechniky. Zařízení by měla být chráněna proti přepětí. V každé důležité místnosti by měl být umístěn hasicí přístroj (pro elektřinu práškový), aby se dalo zabránit požáru a v každé místnosti umístěno protipožární čidlo napojené na automatizovaný hlásicí systém.

4.3 Sít'

Počítačová síť je provozována pro komunikaci a sdílení dat (informací) z jednoho konce světa na druhý v řádu několika sekund. Díky rozdělení sítě na několik menších sítí lze eliminovat výpadky, které by mohly ovlivnit více společností (státy, firmy, města, obce) či obyvatel a odstříhnout je od komunikace do veřejné sítě. Pomocí sítě se dnes dají realizovat různé činnosti jako například sdílení tiskárny či diskového uložení pro více uživatelů v jedné síti, hraní online videoher, komunikovat po telefonu a další. Síť se rozděluje na několik kategorií, především dle jejich velikosti.

PAN (Personal Area Network) – nejmenší forma sítě, propojení na velmi krátkou vzdálenost, například propojení telefonu a hodinek pomocí Bluetooth.

LAN (Local Area Network) – za síť typu LAN se označují velmi malé sítě od běžných domácností, po firemní sítě s více objekty propojených dohromady v jeden celek.

MAN (Metropolitan Area Network) – jako sítě MAN se označují ty, které spojují více lokálních sítí, typicky více domácností, firem, které mohou být v oblasti jednoho města, případně přilehlých oblastí.

WAN (Wide Area Network) – spojení dvou a více MAN sítí vede k celku, který se nazývá WAN. Tyto sítě spojují velká města, státy, či kontinenty.

Celá síť se skládá z několika komponentů (aktivní a pasivní síťové prvky). Nejdůležitějším prvkem je router a propojovací kabeláž. Kabeláž spojuje jednotlivé sítě dohromady a router předává (směřuje) komunikaci na další router (směrovač). Aby jakýkoliv prvek v počítačové síti mohl komunikovat, musí být připojený a mít možnost být identifikován (IP adresa, MAC adresa).

V rámci propojení poboček je důležité zmínit možnost virtuální sítě neboli VPN (Virtual Private Network). Princip fungování VPN je vytvoření tzv. tunelu mezi jedním a druhým místem (např. centrála a pobočka). Slouží k propojení dvou sítí typu LAN skrze síť Internet. Komunikace v této privátní síti je šifrovaná a tím pro ostatní prvky na síti nečitelná.

VPN může sloužit pro více účelů. Nejčastější použití je v soukromé sféře pro vzdálený přístup a ochranu uživatele, aby se o něm poskytovatel internetu a poskytovatel webových stránek nedozvěděl více informací, než je nutné. Případně je využíván v podnikové sféře pro vzdálený přístup k firemnímu serveru např. z domácího prostředí.

V případě problematiky propojení např. dvou poboček je ale situace trochu odlišná. Zde se používá VPN typu site-to-site, ve které se propojí router jedné pobočky s routerem druhé pobočky. Pro zajištění zabezpečeného spojení těchto routerů se používají nejrůznější protokoly. Aktuálně nejvíce používaný protokol IPsec, který nabízí pokročilé šifrování. Tento protokol šifruje každý jednotlivý paket a zajišťuje bezpečnost přenosu dat po internetu. [6]

5 Microsoft 365 + Azure

Microsoft 365 je balík cloudových aplikací určených převážně pro podniky. Platforma „Microsoft Azure je cloudové prostředí určené k vytváření a běhu hostovaných a škálovatelných serverů, aplikací a dalších služeb. V Azure lze provozovat scénáře v prostředí: IaaS (Infrastruktura jako služba), PaaS (Platforma jako služba) i SaaS (Software jako služba). Microsoft Azure tak lze popsat jako neustále se rozšiřující sadu cloudových služeb, které pomáhají jakékoliv organizaci překonávat překážky v podnikání. Nabízejí svobodu při sestavování, správě a nasazování aplikací v rozsáhlé globální síti pomocí oblíbených nástrojů a architektur.“ Převzato z [7]

Obě služby jsou dodávány jako SaaS (Software as a Service), tedy uživatel si nekupuje doživotní licenci, ale službu, za kterou platí na měsíční nebo roční bázi. Nikdy nic není vlastněno koncovou firmou, ale je to dodáno jako služba včetně cloudu s tím, že nemusí být použité žádné vlastní on-premise (lokálně instalované) řešení. S nákupem první uživatelské licence Office 365 je získán vlastní tenant (viz kapitola 5.1) na úrovni podle použité licence. Ten běží na Azure jako Cloud Computing (program, který je pronajímán uživatelem/firmou). Díky tomu je umožněn přístup k serverové straně, jakožto Microsoft Exchange Server (poštovní server), Microsoft SharePoint Server (viz kapitola 5.4). Azure Active Directory (viz kapitola 5.2), Endpoint Manager (produkt pro komplexní správu koncových zařízení) a dalším službám, bez kterých by řešení nemohlo fungovat. Na toto navazuje škálovatelnost služeb. Za předpokladu, že by se společnost rozšířila a měla dostatečný počet uživatelů s vyššími licencemi, tak bude obdržen přístup k vyšší licenci Azure Active Directory a bude možno použít další funkce, jako podmíněné šifrování dokumentů, kontrola ochrany údajů, auditování přístupů a další věci, ke kterým by se v on-premise řešení musely nakupovat velmi drahé licence. Vždy záleží na velikosti firmy, počtu uživatelů a konkrétní potřebě k určení, zda zvolit on-premise řešení nebo cloud. Přestože služby běží v cloudu, je možné se k většině modulů připojit pomocí příkazové řádky Power Shell a jednat s

nimi, jako by byly on-premise (lokálně instalované), protože ne všechna nastavení je možné provést pomocí webového rozhraní. [8]

IT jako služba (ITaaS) je služba poskytovaná z centralizovaných datových středisek. Tato služba zajišťuje výkonný hardware, který může firma používat po síti a nemusí jej vlastnit. Jedná se o infrastrukturu distribuovaných datových center propojených skrze IP (Internet Protocol) síť. Stojí za zmínku třívrstvá cloudová architektura, která v sobě zahrnuje dodání aplikací do nejvyšší vrstvy, propojení (rozhraní) mezi operačním systémem a sítí, aby se mohly využívat veškeré cloudové aplikace. [9]

Tyto služby jsou užívané prostřednictvím internetu jako běžná internetová aplikace. Doba se posouvá a tradiční IT služby jsou již skoro zapomenuty. Nahrává tím cloudovému řešení, které se zdá být pro budoucnost firmy výhodnější než tradiční řešení, především z důvodu vyšších investic jak za software, hardware, tak potřebný vyškolený personál, který se stará o údržbu. Výhodou využívání cloudových služeb je úspora finančních prostředků, díky kterým dokáže firma lépe optimalizovat své fixní náklady. Mezi takové patří např. hostovaná služba Microsoft Exchange Online, která dokáže kdykoliv a komukoliv poskytnout přístup k emailovému klientovi, kalendáři, či kontaktům z vícero zařízení.

Ceny v březnu 2022 zlehka stouply oproti těm dřívějším. Za jednoho uživatele služby Microsoft Exchange Online firma aktuálně zaplatí necelé 4 dolary měsíčně. V případě, že chce uživatel využívat i desktopových (aplikace instalovaná na lokálním disku, vázaná na operační systém) aplikací, vyjde to celkem na necelých 12 dolarů měsíčně za jednoho uživatele (březen 2022).

5.1 Tenant

Pojem tenant (z anglického „nájemník“) je v rámci služeb Microsoft 365 jedinečným prostorem organizace sdružující všechny jednotlivé služby (Azure AD, Exchange, SharePoint a další).

Při zakládání tenantu je třeba vytvořit vlastní unikátní název, který jej bude vždy provázet. Je neměnný a bude se objevovat v URL adresách, kupříkladu https://nazev_tenantu.sharepoint.com. Co organizace, to jeden tenant.

5.2 Azure Active Directory

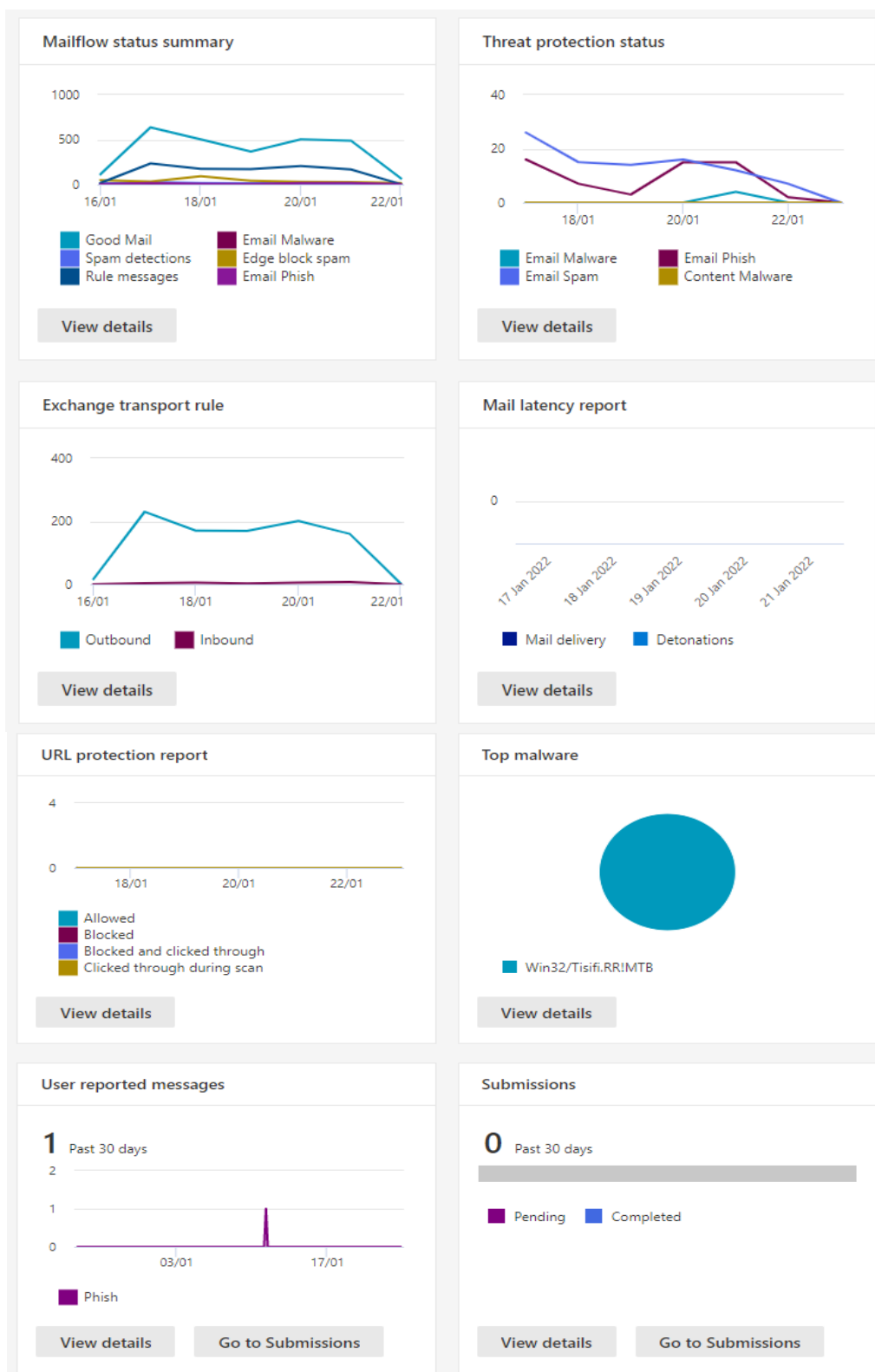
Azure Active Directory [10] je obdoba on-premisového Active Directory, který funguje jako služba na Windows Serveru. Označení Azure vyjadřuje, že se jedná o cloudový AD (Active Directory), který je provozován v datacentrech Microsoftu. Za předpokladu, že by již byl ve firmě v provozu lokální Active Directory, je možné jej synchronizovat s Azure, mít redundanci a provozovat hybridní řešení. Azure Active Directory se používá pro správu, identifikaci, ověřování a přistupování jednotlivých uživatelů.

Active Directory je databáze uživatelů, počítačů, skupin a serverů. V rámci organizace funguje jako správce identit. Dále se propojuje s dalšími rolemi využívající Active Directory. Nejčastěji je v rámci on-premise využíván s funkcí Group Policy, která správci umožňuje přidělovat specifická práva pro celou strukturu či pro individuálního uživatele. Pokud by se spolupracovalo s jinou společností, je možnost vytvořit federaci, která zajistí vzájemnou důvěryhodnost.

5.3 Exchange Online

Exchange Online je cloudová obdoba on-premisového Microsoft Exchange Serveru, ale jeho součástí je Exchange Online Protection, který obsahuje antivir, antispam a další zabezpečovací funkce. Často se používá i samostatně v konfiguraci, kdy firma má pouze on-premise infrastrukturu, ale přesto využívá Exchange Online Protection jako ochranu dat a zaměstnanců před hackerskými útoky. Je schopný se učit, předkládat emaily k revizím a přesouvat do karantény. Hlavní výhoda Exchange Online spočívá v tom, že funguje na serverech Microsoftu s vysokým výkonem. Není třeba se tedy obávat toho, že přijde hackerský útok, typicky tzv. DDOS útok zahlcující síť mnoha požadavky, který by Exchange kompromitoval a odříznul celou společnost od emailové komunikace. [11]

Na obrázku (viz Obrázek 1) je vidět jednoduchý zkrácený přehled z konzole, kde lze sledovat statistiky, aktuální hrozby, co je nejčastěji blokováno, případně na jaké uživatele útok cílí nejčastěji.



Obrázek 1 Exchange online, zdroj vlastní zpracování

5.4 SharePoint

Softwarový nástroj SharePoint se používá jako knihovna korporátních dokumentů a pro firemní weby (intranet). V rámci firemních webů je možno s kolegy sdílet nejrůznější informace, články, jednoduché webové aplikace a za pomoci dynamických součástí webů je možno zobrazovat např. události z celofiremního kalendáře, různá hlasování a počasí. [12]

Velikost dostupného úložiště na SharePointu se určuje podle počtu uživatelů. V rozhraní pro správce SharePointu se mohou zakládat jednotlivé weby, které mohou kategorizovat obsah. Ke každému webu může být vytvořen tým v aplikaci Teams a složka ve službě SharePoint. K nim poté uživatel může přistoupit přes webovou stránku SharePoint nebo přes klientskou aplikaci OneDrive. Přístupy k souborům lze definovat na jednotlivé uživatele či security groups (skupiny zabezpečení). [12]

Klientská aplikace OneDrive má výhodu, že je multiplatformní a například v prostředí Microsoft Windows jsou poté všechny dokumenty dostupné, jako kdyby byly uloženy lokálně na disku, ale přesto nezabírají prostor a při úpravách se synchronizují s ostatními uživateli.

Nespornou výhodou dokumentové knihovny SharePointu je tzv. koš druhé úrovně, ze kterého může správce obnovovat soubory uživatelů, které byly odstraněny z koše první úrovně. Pokud uživatel udělá chybu v úpravě dokumentů, není problém pomocí verzování souborů obnovit jeho minulé verze.

5.4.1 OneDrive

Další službou sady Microsoft 365 je osobní úložiště OneDrive, které uživateli nabízí jeden terabyte prostoru pro osobní data v rámci firmy. Přestože je OneDrive prezentován jako separátní služba, na pozadí je provozována na SharePointu. Odlišuje se tedy tím, že soubory na SharePointu jsou určeny pro skupiny lidí, OneDrive je čistě osobním prostorem zaměstnance. Jeho data se taktéž synchronizují skrze klienta OneDrive a je možné je sdílet s vybranými spolupracovníky.

5.5 Teams

Aplikace Teams je nástupcem aplikace Skype for Business. Největší rozšíření přišlo s dobou vypuknutí pandemie COVID-19. V danou chvíli bylo velmi rychle potřeba co nejvíce služeb a procesů dostat do online prostředí, aby mohli zaměstnanci začít pracovat z domova a studenti se distančně vzdělávat. Přestože hlavní výsadou Teams je možnost pořádat videokonference, její využití je mnohem rozmanitější. Aplikace má sloužit jako centrální rozhraní většiny služeb Microsoft 365.

Jedná se primárně o vnitrofiremní komunikační nástroj, kde výměnu emailů mezi zaměstnanci nahradil skupinový chat a posílání příloh nahradilo sdílení souborů přes SharePoint. V aplikaci Teams zaměstnanci komunikují napřímo mezi sebou nebo ve skupinových týmech. Součástí týmu jsou jednotlivé diskusní kanály. Týmové soubory se ukládají na společné úložiště SharePoint. V rámci týmu mohou uživatelé nadále využívat např. plánovače úloh, společné kalendáře a hromadné schůzky. Účelem popisovaného prostředí je, aby si uživatel nemusel instalovat všechny klientské aplikace, naopak aby mohl vše obsloužit v rámci jednotného webového prostředí.

6 Síťová infrastruktura

Firemní síť je základním komunikačním prostředím a je nezbytné, aby její návrh byl dokonale propracovaný pro pokrytí služeb stávajících a dovoval další rozšíření. Důležité je mít síť dobře naplánovanou a rozdělenou na menší segmenty (tzv. VLAN) [13]. Tyto virtuální lokální sítě zajišťují oddělení sítě tak, aby se hosté nemohli dostat k datům a komunikaci v LAN síti, která s jejich činností nijak nesusouvisí. Například je nutné zajistit, aby se hosté nedostali do VLAN, skrze kterou se konfiguruje síťová zařízení. Vzhledem k tomu, že je snahou dělat vše kompletně škálovatelné, daná síť by se měla držet nějakého řešení SDN (Software Defined Network). Pomůže to předejít nákupu levnějších zařízení a jejich pozdějšímu nahrazování. Zároveň později nebude nutné obsluhu školit na novou síť.

6.1 Virtualizace

Při budování firemní serverové a síťové infrastruktury vhodném se neměla přehlédnout nepřehlédnout technologie virtualizace. Jak již název napovídá, za pomoci různých virtualizačních platforem (Microsoft Hyper-V, VMWare ESX, CitrixXenServer, Proxmox a dalších...) je možno na jednom, či více virtualizačních fyzických serverech (hypervizorech) spustit více serverů virtuálních.

To po technické stránce umožní lépe využít výkonový potenciál fyzických serverů přítomných ve firmě. Správce má snadnější správu a pro nepřetržitý běh důležitých firemních aplikací je možné více serverů spojit do tzv. clusteru, který umožní nepřetržitý běh virtualizovaných serverů v případě selhání jednoho z fyzických serverů. [14]

Po ekonomické stránce přináší využití některé z virtualizačních platforem ekonomické výhody. Není třeba nakupovat a spravovat více fyzických serverů včetně záruk na jejich servis, šetří se energie (jak kvůli chlazení serverovny, tak z důvodu efektivnějšího zatížení menšího počtu serverů) a taktéž se ušetří finanční prostředky za nákup licencí na provozované operační systémy.

6.2 Poskytovatel internetových služeb

Při výběru poskytovatele těchto služeb je prvotně třeba zohlednit, jací poskytovatelé internetu v daném místě poskytují připojení k síti Internet. Jelikož je dnes většina služeb využívána v cloudu, měla by být přípojka dostatečně dimenzována, aby byla její kapacita dostačující i v případě navýšení požadavků na provoz. Samozřejmostí by měla být i redundantní (záložní) linka a veřejná IP adresa. Díky veřejné IP adrese může firma publikovat služby své infrastruktury do sítě Internet. [15]

Je složité určit, co znamená dostatečně dimenzovaná linka. Je možné spočítat a předpovídat tak budoucí provoz na základě počtu uživatelů, serverů a počtu používaných aplikací online. Správným krokem je domluva s poskytovatelem internetu na nějaké požadované rychlosti, která odpovídá počáteční kalkulaci a nadále možnost jej poté v reálném provozu upravit (snížit či navýšit).

V místě sídla firmy by bylo vhodné najít poskytovatele internetu, který nabízí připojení po optickém kabelu, alternativně rádiovým spojem ve vyhrazeném pásmu. Pokud není ani jedna z variant možná, lze připojení realizovat bezdrátovým spojem ve volných pásmech, po telefonním rozvodu (xDSL) nebo po bezdrátové síti mobilního operátora. [15]

6.3 Aktivní síťové prvky

Aktivní síťové prvky jsou ty, které digitální signál nějak upravují a modifikují ho, kupříkladu tedy switch, router, AP (Access Point), server, repeater (opakovač signálu) rozbočovač a podobně. Nazývají se aktivní, protože se reálně podílejí na komunikaci na rozdíl od kabeláže, kterou jen prochází signál, ale není nijak modifikován či zesilován.

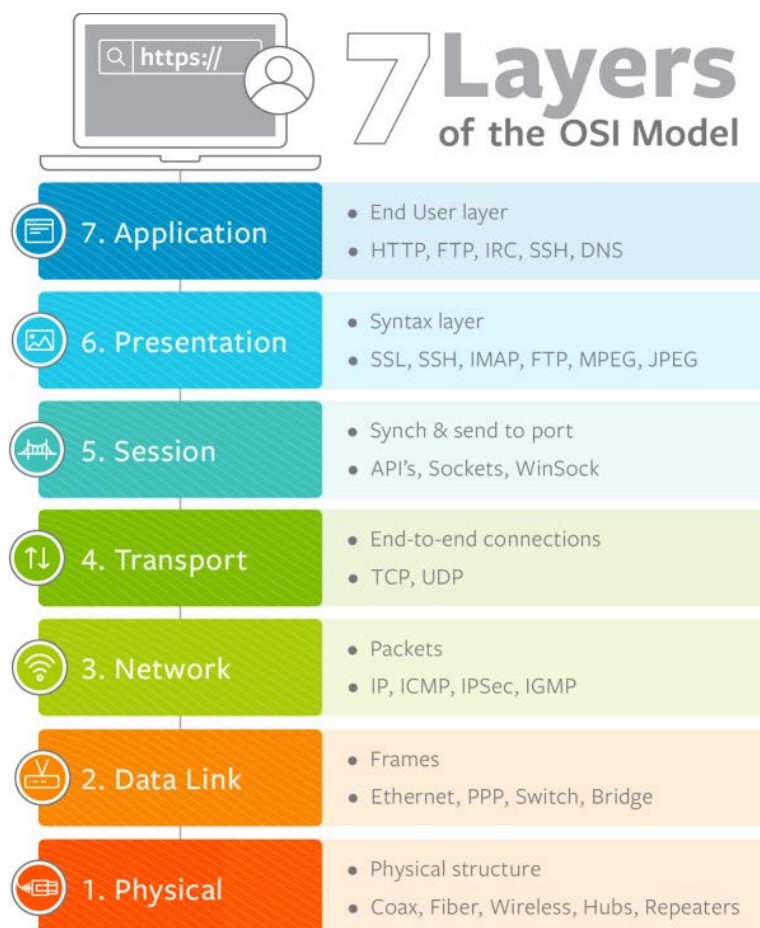
6.3.1 Router a Firewall

Router [16], jakožto chytré zařízení, je označován za aktivní prvek v síti. Pracuje na 3. vrstvě OSI modelu (novější pracují na 7. vrstvě), kde se k přenosu datových paketů využívají IP protokoly. OSI model [17] je standardizovaný souhrn norem, který představuje náhled na jednotlivé vrstvy sítě (viz Obrázek 2). OSI model byl vytvořen k jednoduššímu pochopení, jak celý proces probíhá, jak funguje síť, z čeho všeho se skládá a které jednotlivé vrstvy v jakém pořadí musí spolupracovat, aby byla zajištěna správná komunikace. Každá nadřazená vrstva se vždy odkazuje na nižší vrstvu, kterou používá pro své další procesy.

Router má za úkol proces, kterému se říká routování (směrování). K tomu se potřebné informace ukládají do routovací tabulky. Router funguje jako prostředník mezi veřejnou sítí a lokální sítí. S jeho pomocí lze také spojit dvě lokální sítě nebo jinou vzdálenou síť.

Samotné směrování může probíhat staticky nebo dynamicky. Pokud neexistuje předem nadefinovaná cesta, řídí se defaultním nastavením. Statické směrování se používá u velmi malých sítí, kde se počet prvků pohybuje v řádu jednotek až nižších desítek. Pro rozsáhlejší sítě je využíváno dynamické směrování, které rychle a automaticky reaguje na každou změnu v síti. Lze zmínit nejčastěji užívané směrovací protokoly, a to nejstarší RIP (Routing Information Protocol),

který je používán v menších sítích a je nejjednodušší pro konfiguraci; středně pokročilý, určený pro větší sítě OSPF (Open Shortest Path First) a routovací protokol BGP (Border Gateway Protocol), které se využívá u větších sítí, jako jsou propojení mezi ISP (Internet Service Provider).



Obrázek 2 OSI model, zdroj: [18]

Router také umí zajišťovat dynamické přidělování IP adres koncovým zařízením tak, aby každé zařízení vždy obdrželo správnou IP adresu. IP adresy lze případně přidělovat ručně – staticky.

Další důležitou funkcí je tzv. NATování, které souvisí s firewallem. Tato funkce routeru překládá síťové adresy z veřejného adresního prostoru do vnitřního a naopak. NAT (network address translation) se začal využívat z důvodu nízkého množství veřejných IPv4 adres. Jednoduše celá vnitřní síť posílá informace do vnější sítě přes jednu adresu. Pro IPv6 se již NAT nevyužívá.

Firewall zajišťuje ochranu vnitřní sítě a může být samostatným zařízením nebo může být integrován do routeru. Jeho úkolem je blokovat požadavky, které

nejdou povolené. Nejlepší metodou, jak ochránit síť, je zakázat veškerý provoz a poté povolit služby a porty, které jsou IT správci známé. Firewall je další prostředník mezi lokální a venkovní sítí, který se stará o bezpečnost. Firewallem prochází veškerá komunikace na síti a je to jediná cesta, kterou může daný paket projít zvenku či zevnitř, a tudíž jej na základě definovaných pravidel zkontroluje a buď povolí, či zamítne vstup do vnitřní sítě nebo naopak. Mimo výše popsaného firewallu existuje varianta pro koncová zařízení (notebooky, PC), která filtruje provoz na úrovni jednoho zařízení a bývá instalována společně s dalšími bezpečnostními prvky. Některé dnešní firewally umí i DPI (Deep Packet Inspection) a jsou schopné vyhodnocovat hrozby už za provozu, např. nebezpečné útoky schované v běžném provozu. Firewall nemusí vždy sloužit pouze k ochraně vnitřní sítě, dá se využít pro určitou formu cenzury na internetu, typicky jsou zakázána určitá slova. Firewall působí obousměrně. Nechrání jen tu komunikaci, která přichází zvenku do lokální sítě, ale zajišťuje, že i naopak do veřejné sítě nebude odcházet škodlivý kód, kterým byl třeba dříve počítač infikován. Před každou implementací síťového prvku, jako je router či firewall, je třeba si definovat, k čemu je takové zařízení potřeba, jaké jsou požadavky firmy (hlavně na bezpečnost), jaké jsou možnosti investice, co od toho řešení očekávají, jaký je očekávaný růst firmy do budoucna. Je třeba provést prvotní analýzu a poté přemýšlet nad tím, zdali se bude implementovat softwarové řešení firewallu, firewall integrovaný do routeru, či fyzický firewall jako samostatný síťový prvek. Parametry firewallu, které je nutné zvážit, je výše zmiňovaná bezpečnost, maximální propustnost, kompatibilita s IPv6, v případě HW řešení počet a typ portů k propojení, možnost redundance a případný servis. [19]

V souvislosti se síťovými prvky je důležité zmínit službu ACL (Access Control List) [20]. Tato funkce routeru umožňuje automaticky filtrovat provoz. Pracuje se souborem definovaných pravidel a dle nich kontroluje příchozí i odchozí pakety. Paket buď předá dál, či zablokuje. Funkce ACL je používána především pro bezpečnost a zajišťuje větší kontrolu nad spravovanou sítí. Pokud IT správce špatně nakonfiguruje ACL, může to mít negativní dopad na celou síť, který zapříčiní nefunkční spojení.

6.3.2 Switch

Switch je aktivní síťový prvek starající se o rozdělení sítě na více částí. Dají se definovat 2 základní typy switchů. Unmanaged a managed. Unmanaged jen „rozbočují“ síť na další porty bez ohledu na VLANy. Umístění jednotlivých zařízení v síti si zapamatovávají pomocí tabulky MAC (Media Access Control) adres, kterou si sami generují od svého posledního startu. MAC adresa je jasně definovaná adresa, která je přidělená síťovému prvku bezprostředně po jeho výrobě.

S managed switchi lze již provádět určitou interakci, nejčastěji mají webové rozhraní a je možné definovat VLANy, trunk porty a využívat další funkce jako detekce smyčky či detekce zapojení neautorizovaného DHCP (Dynamic Host Configuration Protocol) serveru.

6.3.3 Access Point

Jedná se o aktivní síťový prvek sloužící k bezdrátovému připojování koncových zařízení do sítě. Ve firemním prostředí se používá ve většině případů jen k propojení ethernetového média s bezdrátovým. Nestará se tedy o přiřazování IP adres, směrování, ani další funkce, které jsou řešeny jinými prvky. Access Point umožňuje skenovat ostatní síť, zachytávat bezdrátové útoky a pokročilejší AP se dokážou příchozím útokům aktivně bránit. [21]

6.3.4 Kamerový systém

V roce 2022 již proběhla modernizace i v oblasti kamerových systémů. Většinou se kamerový systém skládá ze samotných kamer a NVR (Network Video Recorder). NVR je zařízení, které se stará o provoz, ukládání nahrávek a jejich zpracování. Kamerový systém posílá data po síťovém rozhraní. Pro výběr kamerového systému je klíčové vhodné rozlišení dle požadovaného použití. [22] Je vhodné volit rozlišení Full HD a vyšší. Kamerový systém je využíván především pro kontrolu a jako prevence. V případě potřeby kvalitního záběru se bez patřičného rozlišení nelze obejít. Je proto vhodné dopředu uvažovat nad funkcí WDR (Wide Dynamic Range), která dokáže přispět ke kvalitnějšímu obrazu a rozeznávání předmětů či osob na kamerovém záznamu. Rozlišují se především 2 typy objektivů. Varianta s pevnou ohniskovou vzdáleností, kde je omezení na základě prvotního nákupu, či lepší variantou jsou kamery s optickým zoomem, které umožňují nastavení ohniskové

vzdálenosti. Vhodnou funkcí kamerového systému je automatická detekce pohybu, která se dá provázat s automatickým sepnutím nahrávání, nebo spuštěním alarmu. Jednou z variant je využití kamerového systému od společnosti Hik Vision, jehož pořizovací náklady jsou okolo 20 tisíc Kč a zároveň splní všechny základní a středně pokročilé požadavky. Investovat lze také do nákladnějšího řešení, například od značky Ubiquiti, které bude mít podporu AI (Artificial Intelligence) učení, bude umět rozpoznávat obličeje, zaznamenávat na časové ose pohyb, posílat upozornění a kontrolovat docházku.

6.3.5 Software Defined Network Controller

Jelikož je celé řešení směřováno na SDN (Software Defined Network), tak musí mít i nějakou inteligenci, která se bude starat o kompletní zastřešení a nastavování jednotlivých síťových prvků. Vhodným produktem je třeba Ubiquiti UniFi Cloud Key, případně může být controller (zařízení pro nastavení síťových prvků) integrován do routeru, jako například Ubiquiti UniFi Dream Machine Pro, nebo může běžet samostatně na aplikačním serveru např. linuxovém.

Pokud je daná síť spravovaná nějakým controllerem, tak je celá její konfigurace uložena do něj a ten se stará o vytváření konfigurace a distribuci do jednotlivých síťových prvků. Ačkoliv toto řešení může znít jako single point of failure (jediný bod selhání), u většiny výrobců jsou prvky schopné fungovat bez nepřetržitého přístupu ke controlleru, protože v sobě mají uloženou poslední konfiguraci.

SDN se začalo dostávat do povědomí z důvodu reakce na trh. Všechno se zrychluje, modernizuje a je třeba tomu přizpůsobit i danou technologii. Za předpokladu, že chtějí firmy využívat všechny trendy jako IoT (Internet of Things), vysokorychlostní internet a další služby, tak musí proběhnout významný upgrade síťové infrastruktury. Již od počátku vzniku internetu bylo zřejmé, že skýtá velké nedostatky. Šlo o to, že již okolo roku 2003 bylo na trhu spousta opatření, jak chránit infrastrukturu, bohužel jich bylo tolik, že neměla rozumný a kvalitní základ. Chyběl ucelený systém, který by toto zajišťoval, proto řada univerzit začala pracovat na výzkumu softwarově definovaných sítí. Svět do té doby znal router, switch a další zařízení pouze v běžné podobě. [23]

„Tím, že se oddělila řídicí rovina od datové roviny, umožnilo spouštět řídicí rovinu softwarově, na standardních serverech a umožnilo tak snadno vytvářet nové virtualizované řadiče a služby na míru. To umožnilo agilní a optimalizovaný provoz prostřednictvím programování sítě, spíše než se uchýlit k ruční konfiguraci prostřednictvím nízko-úrovňových rozhraní.“ Převzato z [23]

Díky tomu všemu se docílilo vyšší rychlosti systému, který dokáže rychle reagovat na změny. Postupný vývoj ukazoval, že celé IT se bude uchylovat k softwarově definovaným sítím. Hlavní výhodou SDN je dynamika, kdy se celé prostředí velmi rychle modifikuje a přizpůsobuje podmínkám, dále velmi dobrá škálovatelnost či jednoduchá správa celého systému. V obecné rovině je SDN nutností, když se celá populace pomalu ubírá směrem Cloud Computingu, všechny služby a produkty, včetně dat, se přesouvají do cloudu. [23]

Již v roce 2013 mnozí věděli, že SDN je budoucnost a má velký potenciál. Dnes se opravdu dá říct, že vize z roku 2013, se stala realitou a střední firmy využívají primárně SDN a cloudové služby. [23]

„Vlastnosti cloud computingu jsou:

- *Více nájmovost (Multitenancy) – konkrétní fyzické zdroje jsou sdíleny mezi více uživateli*
- *Průběžný systém placení (Pay as you go) – uživatel platí za to, co reálně využije*
- *Aktuálnost (Up to date) – veškeré aktualizace a upgrady provádí poskytovatel*
- *Škálovatelnost a výkonnostní elasticita (Scalability and performance elasticity) – uživatelům dovoluje jednoduše změnit zdroje a služby.“* Převzato z [24]

6.3.6 Network Attached Storage (NAS)

Takzvaný NAS je jednoduché inteligentní zařízení, které umožňuje zálohu fotografií, videí či jiného datového obsahu firmy a jeho následné sdílení po síti. K datům se většinou přistupuje skrze webové rozhraní. Použitelnou kapacitu pro uložení dat ovlivňuje počet a velikost vložených diskových jednotek a využití jedné z metod typu RAID (Redundant Array of Independent Disks). RAID je metoda, která se stará o duplikování dat jako opatření proti selhání pevného disku. Umožňuje z vícero fyzických disků vytvořit jeden velký úložný prostor. [25]

NAS je možné využít na zálohy zařízení, případně celého cloudu, pokud by IT správce chtěl určitá data uchovávat lokálně ve firmě. Dá se využít i pro verzování souborů, protože v cloudu se verze neukládají napořád. NAS je možné taktéž využít jako webový server. Mezi nejznámější značky lze zařadit Synology nebo Qnap, kdy každé řešení má své pro i proti. Nejvhodnější je určit si, kolik dat je třeba v NAS uchovávat a podle toho vybrat model s takovým počtem pozic na disky, která bude odpovídat požadované kapacitě a metodě zabezpečení RAID. Je velmi důležité kupovat pevné disky vždy zvlášť a alespoň po skupinách od jiných dodavatelů. Jedině tím se lze vyhnout potencionálnímu problému, že by některý výrobce měl vadnou celou šarži a nemělo by se tak stát, že se všechny disky pokazí například v rozmezí jednoho dne. Pokud jsou ve firmě požadavky pro rychlejší práci, je možné vybrat model, který bude mít prostor na SSD disk a bude zrychlovat ukládání dat. Samozřejmě neméně důležitou roli hraje vhodná konfigurace RAID, která určuje, jak rychlé bude výsledné úložiště a jak bude odolné proti kolapsu a ztrátě dat. Pro středně velkou společnost by mohl být vhodný NAS se čtyřmi pozicemi a pozicí navíc pro SSD akceleraci, k tomu 4× 4 TB disky a na celek aplikovat RAID 5, získat tím cca 12 TB prostoru a mít poměrně dobrou rychlost čtení. Nevýhodou může být, že lze ztratit pouze jeden disk. Vzhledem k tomu, že by NAS v kombinaci s využitím cloudových řešení měl sloužit pouze pro „jistotu“ a archivaci dat, neměla by firmu případná ztráta daných dat omezit. Výběr je vždy velmi individuální a závisí na požadavcích a potřebách firmy. Jednotlivé možnosti konfigurace RAID jsou znázorněné v přehledné tabulce níže (viz Obrázek 3).

Disková pole RAID

Typ svazku	Počet disků HDD	Tolerovatelný počet závad disků	Popis	Kapacita svazku
Základní	1	0	- Skládá se z jednoho disku jakožto nezávislé jednotky. - Neumožňuje redundanci dat.	1 x (velikost disku HDD)
JBOD	≥ 1	0	- Jednotlivé disky seskupuje do jednoho úložného prostoru, jehož kapacita se rovná součtu kapacit jednotlivých disků. - Neumožňuje redundanci dat.	Součet velikostí všech pevných disků HDD
RAID 0	≥ 2	0	- Obsahuje funkci „proužkování“, proces, při kterém jsou data rozdělena do bloků a tyto bloky rozmístěny na více discích, což zvyšuje výkonnost. - Neumožňuje redundanci dat.	Součet velikostí všech pevných disků HDD
RAID 1 (zrcadlení)	2	1	- Souběžně na oba disky zapisuje stejná data. - Umožňuje redundanci dat.	Velikost nejmenšího disku HDD
	3	2		
	4	3		
RAID 5	≥ 3	1	Zavádí funkci proužkování dat na úrovni bloku s paritou, kdy jsou data rozmístěna napříč všemi začleněnými disky, díky čemuž je redundance dat účinnější než u typu RAID 1.	$(N - 1) \times$ (velikost nejmenšího pevného disku HDD)
RAID 6	≥ 4	2	Zavádí dvě vrstvy parity dat umožňující uložení redundantních dat v objemu odpovídajícím velikosti dvou disků, což znamená vyšší stupeň redundance dat než u typu RAID 5.	$(N - 2) \times$ (velikost nejmenšího pevného disku HDD)
RAID 10	≥ 4 (sudé číslo)	Polovina celkového počtu disků HDD	Poskytuje výkon typu RAID 0 a ochranu dat na úrovni typu RAID 1, kdy se disky seskupují po dvou a data se zrcadlí z jednoho disku na druhý.	$(N / 2) \times$ (velikost nejmenšího pevného disku HDD)

Obrázek 3 Disková pole RAID, zdroj: [25]

6.4 Pasivní síťové prvky

Do kategorie pasivních síťových prvků se zařazují různé propojky, kabely, konektory apod. Tato zařízení sama o sobě nevykonávají žádnou činnost, při které by musela o něčem rozhodovat, předávat pakety, směřovat apod. Mohou být skrze ně napájená zařízení jako například AP, switche, kamery. Tomuto standardu pro napájení se říká PoE (Power over Ethernet). Použití PoE zahrnuje mnoho výhod. Případný výpadek elektrické sítě v celé budově danou síť nakonec nijak neomezí, bude nadále funkční a mobilní zařízení budou schopná dále vykonávat svou práci, protože hlavní zařízení v racku (router, switch) budou zálohována pod záložním zdrojem energie. Také není nutné tahat další kabely pro napájení. Vznikne úspora na kabeláži, zásuvkách, průrazech a s tím spojené práci. Nevýhodou může být vzdálenost mezi prvky. Pomocí PoE lze napájet AP, IP kamery, IP telefony.

6.4.1 Rack

Rack bývá většinou umístěn v technickém zázemí a užívá se pro přehledné uložení všech prvků firemní sítě. Standardní rack je 19" a jeho pozice se určují na tzv. U. 1U je 43,66 mm. [26] Příkladem může být switch, který mívá nejčastěji rozměr 1U, na druhé straně třeba server může mít klidně 4U. Při jeho výběru je velmi důležitá jeho ideální velikost, tedy aby se tam všechna zařízení vešla jak na výšku, tak

hloubku. Určitě je dobré myslet na rezervu, a hlavně na doplňky pro organizaci kabeláže (cable management). Důležitým aspektem je přehlednost. Rack by měl mít zaslepené volné pozice pro oddělení chladné části od teplé tak, aby se teplý vzduch zepředu odváděl dozadu a necirkuloval dokola. Rack pro síťové prvky by měl mít integrované aktivní chlazení, který monitoruje teplotu a dle toho přizpůsobuje otáčky ventilátorů. Obecně je vždy lepší volit větší rack, kde se dané prvky a kabeláž lépe organizují a zároveň bude takový rack připravený pro případný upgrade síťové infrastruktury.

6.4.2 Strukturovaná kabeláž

Kabeláž je nedílnou součástí všech síťových prvků. Je složité určit, co je rozumné řešení s ohledem na budoucí vývoj. Jestli bude všude natažen kabel kategorie Cat 5e, který je nejrozšířenější, používaný mnoho let a v dnešní době bez problému zvládá přenosovou rychlost až 1Gbit/s, nebo jestli všude využít optické kabely. Použitím optických vláken se dá 100% pokrýt budoucí rozvoj, ale zase bude stát nemalé peníze jejich připojení ať už do síťových prvků, nebo koncových stanic. V případě, že je nutné připravit strukturovanou kabeláž na vlastní náklady, jelikož ve firemním objektu není připravena, tak je vhodné tahat kabel kategorie Cat6a, který vychází nejlépe v závislosti na poměru cena/výkon/budoucnost. Cena tohoto kabelu je cca 15 Kč/m, přitom zvládne až 10Gbit/s. Jeho zakončení musí být provedeno vždy v patch panelu nebo keystone (speciální konektor), tudíž není možné jej ukončit standardním konektorem, ale to by mělo být dnes normou v každé nové instalaci. Problémem může být souběh těchto kabelů se silovým vedením. Technologie naštěstí dost pokročily a tento nežádoucí efekt zvládají bez větších problémů. Pro smysluplnou kabeláž je zcela nutné mít v patch panelu označenou konkrétní trasu pro detekování, kde se nachází druhý konec kabelu a k čemu je využíván. Označená trasa musí být jednoduše a rychle dohledatelná.

Kabeláž založená na optických vláknech se dnes užívá především pro páteřní spoje. Optické kabely nejsou tolik náchylné na vnější vlivy, ale není možné je ohnout tolik jako metalické. Nejsou elektricky vodivé, tudíž je možné vést je společně se silovým vedením uvnitř budovy bez toho, aniž by se vyskytlo rušení. Po optickém vláknu je možné poslat informace až stovky km, proto jsou používány na velmi dlouhé

vzdálenosti. Lze rozlišit dva typy a to Single-mode a Multi-mode. Bud' jednovidové nebo vícevidové optické vlákno (vid = paprsek). Při použití těchto vláken se rozlišuje vlnová délka a průměr jádra optického vlákna. Single-mode optická vlákna se používají spíše pro dlouhé vzdálenosti (desítky až stovky km), kdežto Multi-mode využijeme spíše v lokální síti pro kratší vzdálenosti (vyšší desítky metrů).

6.5 Firmy a technologie síťových prvků

V této kapitole lze nalézt krátký pohled na výrobce síťových prvků, popřípadě technologie (funkce), které využívají.

6.5.1 Cisco Systems

Cisco Systems, Inc. je počítačová společnost s dlouholetou historií od roku 1984, zaměřující se na síťová řešení. Společnost taktéž zajišťuje certifikované školicí online kurzy CCNA pro střední a vysoké školy, které vychovávají nové IT profesionály. Cisco si zakládá na pravidelném licencování svých produktů. Konkrétně svého vlastního proprietárního (software uzavřeným kódem) operačního systému IOS (Internetwork Operating System). Má portfolio produktů pro všechny oblasti síťové infrastruktury pro podnikovou klientelu. Aktuálně v oblasti síťových prvků propaguje síťové prvky Meraki, které jsou spravovány skrze cloudový přístup.

6.5.2 Ubiquiti Networks

UBNT neboli Ubiquiti Networks, Inc. je společnost, která funguje od roku 2005 [27] a je inovativní společností v oboru síťových prvků, kamer, přístupových systémů a VOIP (Voice over Internet Protocol) telefonie. Začala vyrábět komponenty pro ISP (Internet Service Provider). První bylo zařízení NanoStation v roce 2008, v roce 2009 vytvořili vlastní bezdrátový TDMA protokol AirMax a později v roce 2010 založili řadu UniFi, která byla vyvinuta pro enterprise (korporátní) prostředí. Takže AP, switche, routery s firewallem, kamery a jiné. [28]

6.5.3 Aruba

Aruba, jakožto řešení mateřské společnosti Hewlett Packard Enterprise, vytvořilo odpověď na systém UniFi svojí řadou Instant-On [29]. Jedná se o zařízení typu SDN, které obsahuje pouze switche a AP. Funkce kontroléru jsou implementované v každém zařízení, tudíž je možné je navzájem jednoduše nahradit. Výhodou prvků Aruba je absence controlleru, protože každé zařízení ho má obsaženo v sobě. K obsluze a konfiguraci těchto zařízení stačí pouze chytrý telefon. Nastavení zvládne i osoba bez pokročilých IT znalostí. Tím, že konfigurace sítě je nahraná ve všech zařízeních, tak je zajištěna redundance kompletně celé sítě. Pokud jedno zařízení přestane fungovat, stačí ho nahradit, potvrdit jeho výměnu v aplikaci a vše je opět funkční. Svojí jednoduchostí je odkázáno na menší společnosti, penziony, kavárny a maloobchody. Napájení těchto zařízení je zajišťováno za pomoci standardu PoE.

6.5.4 FortiNet

Prvky od výrobce cílí na pokročilé sítě s důrazem na bezpečnost. Portfolio produktů značky FortiNet zastupuje veškeré cenové kategorie a jsou tak vhodné pro všechny velikosti podniků.

Od malých podniků, přes korporáty, ISP až po datacentra a telefonní operátory. Routery se u značky FortiNet vybírají podle propustnosti. Pokud je požadavkem 50Mbit propustnost včetně všech služeb jako Firewall, IDS, Threat Management a další, musí společnost zakoupit zařízení, co toto umožňuje. Systém je modulární na úrovni služeb, takže si daný správce vybere, co vše chce hlídat a za co je firma ochotná zaplatit. Služby jako DPI na úrovni šifrovaného provozu a antivir se platí na bázi předplatného, kvůli udržování databáze definic.

Výhodné jsou taky pro externí zaměstnance, kterým stačí multiplatformní program FortiClient, do kterého se přihlásí pomocí svého uživatelského účtu a tím jsou schopni se dostat se svým vlastním zařízením do vnitřní sítě a ověřit, zdali je jejich zařízení důvěryhodné. [30] Tím lze ve firmě častěji používat standard moderní doby BYOD (Bring Your Own Device). Při využívání BYOD je vysoký nárok na bezpečnost, který je kompenzován flexibilitou zaměstnanců, a hlavně nižšími náklady firmy na nákup hmotného majetku.

6.5.5 MikroTik

MikroTik je světově rozšířená firma, která svým zákazníkům poskytuje síťové prvky postavené na svém vlastním operačním systému Router OS. Podílí se tak na vývoji vlastního software i hardware. MikroTik taktéž poskytuje certifikované kurzy pod svou značkou MikroTik Academy. Prvky MikroTik nejsou moc využívány pro lokální sítě, ale spíše pro páteřní spoje mezi budovami. Konfigurační prostředí Router OS je velmi intuitivní a rychlé. Nastavení routeru lze udělat během pár minut. Tato firma vyvíjí všechna síťová řešení od malých switchů až po vysokorychlostní routery a vysoko výkonné antény. Původně MikroTik používal specifická zařízení tzv. routerboard, což jsou základní desky, které lze rozšířit o další fyzické moduly jako antény, paměti, sloty a jiné porty. Dnes již tato firma každému svému výrobku říká routerboard.

6.5.6 Intrusion Detection System/Intrusion Prevention System (IDS/IPS)

IDS/IPS je bezpečnostní funkce porovnávající probíhající síťový provoz oproti databázi definic podezřelých spojení a IP adres. Stará se o zamezení přístupu útočníka, nebo alespoň jeho odhalení. Obě služby kontrolují příchozí a odchozí pakety a monitorují neobvyklý provoz na síti. IDS jen kontroluje a upozorňuje, tudíž je nutný zásah člověka, zatímco IPS aktivně do provozu zasahuje.

6.5.7 Deep Packet Inspection (DPI)

DPI se stará o kontrolu provozu. Toto nastává před IDS/IPS, pokud zakoupené zařízení umožňuje DPI. Jedná se o firewall, který umožňuje kontrolu nad OSI modelem ve vrstvě 7. [31] V případě řešení UniFi je IT správce omezen na nešifrované spojení nebo na IP adresy, které jsou veřejně známé či popsány na internetu. Výsledkem může být zobrazení, kdo používá jaké služby a kolik dat spotřeboval. U jiných výrobců, třeba FortiNet, je možné zakoupit licenci na DPI se šifrovaným provozem a poté je možné do kořenových certifikačních autorit přidat certifikát vygenerovaný z routeru. V tu chvíli může router podvrhnout komunikaci a provést řízený Man In The Middle Attack (cílený útok, při kterém se útočník snaží odposlouchávat komunikaci a získat tak citlivá data). Umí taktéž prověřit šifrovaný obsah, tudíž funguje i jako velice pokročilý antivirus.

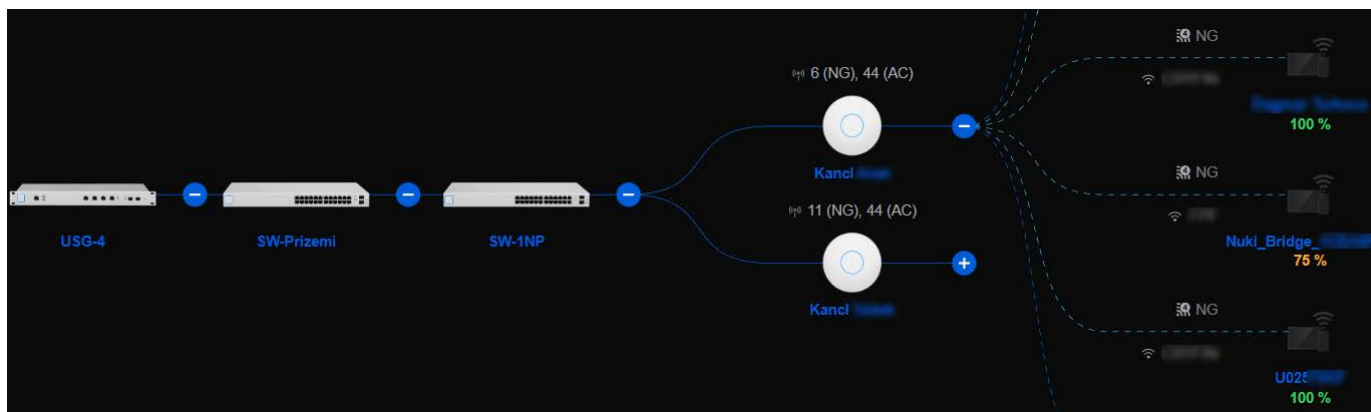
Na obrázku (viz Obrázek 4) je zobrazen přehled přenesených dat za určité období a kam byla tato data přenesena.

Identified Traffic						36.1 KB
NAME		TRAFFIC%	TRAFFIC	DOWN	UP	CLIENTS
Google		41.8%	15.1 KB	6.66 KB	8.45 KB	1
Gmail		23.9%	8.62 KB	3.29 KB	5.33 KB	1
Google API...		14.5%	5.23 KB	2.77 KB	2.46 KB	1
HTTP Prot...		10.7%	3.86 KB	1.78 KB	2.08 KB	1
DNS		9.2%	3.32 KB	3.32 KB	0.00 B	1

Obrázek 4 UniFi DPI, zdroj vlastní zpracování

6.5.8 Controller

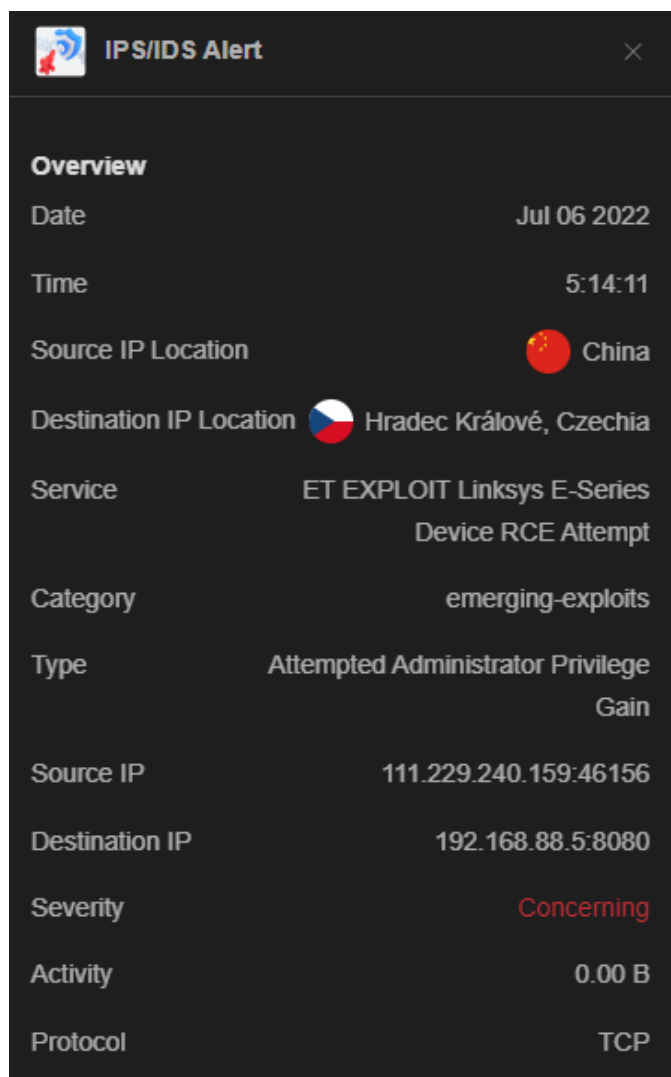
Centrem konfigurované sítě je žádoucí mít controller (kontrolér), ve kterém se vše nastavuje a následně distribuuje do celé sítě. Pokud by chtěl správce přidat další switch, jen ho umístí, na potřebné místo, zapojí, controller ho automaticky detekuje a po povolení přidá do sítě. Každý prvek zná své místo v topologii a pokud na vzdáleném switchi, na určitém portu správce nastaví VLANu, vše se automaticky propíše. Tím adminovi z části odpadá i údržba dokumentace, protože se generuje sama a v jednotném portálu je vidět, kdejaké zařízení je, jaké má IP adresy, na jakém konkrétním portu se nachází, co je zapojeno, v jakém switchi to je zapojeno, a co dále nachází na trase. Na obrázku (viz Obrázek 5) je zobrazena vizualizace reálné topologie z administrativního prostředí kontroléru. Konkrétně ze zařízení UniFi Cloud Key Controller.



Obrázek 5 Topologie sítě UniFi, zdroj vlastní zpracování

6.5.9 Threat Management

Threat Management úzce navazuje na IDS, IPS i DPI. Jde o notifikaci výsledků z těchto systémů, aby pro IT administrátora bylo jednodušší zpracovat všechny informace, provést jejich analýzu a zajistit případná opatření. Kupříkladu u zařízení UniFi se jedná o seznam proběhlých hrozeb, přehlednou mapu odkud útok přišel, označení důležitosti a o co se konkrétně jednalo. Poté může administrátor provést akce jako blokaci zařízení, přesunutí do karantény, prověřit, zdali není kompromitované, případně označit hrozbu jako falešně pozitivní (false-positive). Na obrázku (viz Obrázek 6) lze vidět zaznamenanou hrozbu, vyhodnotit její riziko a podle toho podniknout žádoucí akci. Nejčastěji umístit zařízení do karantény, zablokovat zdrojovou IP adresu, nebo označit jako falešně pozitivní.



IPS/IDS Alert	
Overview	
Date	Jul 06 2022
Time	5:14:11
Source IP Location	 China
Destination IP Location	 Hradec Králové, Czechia
Service	ET EXPLOIT Linksys E-Series Device RCE Attempt
Category	emerging-exploits
Type	Attempted Administrator Privilege Gain
Source IP	111.229.240.159:46156
Destination IP	192.168.88.5:8080
Severity	Concerning
Activity	0.00 B
Protocol	TCP

Obrázek 6 Threat Management, zdroj vlastní zpracování

7 Hardwarové vybavení firmy

Po technologiích, na kterých může být postavena síťová infrastruktura firmy, je nutné představit hardware, který je nezbytnou součástí jakékoliv společnosti. Středně velká firma nad pořízením hardwaru uvažuje více oproti menší kavárně. Jedná se o poměrně nákladné položky, vzhledem k použitému množství. Využití notebooků je v aktuální moderní době nezbytné. Stolní PC jsou využívány minimálně, a to jen pro administrativní pracovníky, kteří mají své pracovní místo pevně určené.

Management a obchodní oddělení využívají již pouze notebooky, jelikož se často vydávají mimo kancelář. Využití tiskárny závisí na potřebách firmy. V případě, že je třeba tisknout mnoho stránek, je dobré si vybrat tiskárnu vhodnou pro firemní použití. Projektory, či televize v konferenčních místnostech jsou samozřejmostí a je zapotřebí, aby měly vynikající zobrazovací schopnosti. Neméně důležitý je výběr drobných periférií, jako je myš a klávesnice. Tyto periferie je třeba vybrat v závislosti na dlouhodobé prosperitě zaměstnanců ve firmě. Spoustě podnikatelů se tyto drobné komponenty jeví jako nedůležitá součást a raději plánují výkonné notebooky, ovšem pokud se zaměstnancům nebude psát na klávesnici pohodlně, firmu to v budoucnu může stát více financí, než úspora v řádu pár stokorun na jedné klávesnici.

7.1 Notebooky

Srdce počítače, tzv. procesor je vyvíjen 2 nejznámějšími společnostmi, a to AMD a Intel. Z dlouhodobých průzkumů společnosti Microsoft vyplývá, že se nejvíce prodávají notebooky postavené na technologii společnosti Intel. Ve výběru by se měl objevit procesor Intel Core i5 a vyšší, kvůli čtyřem fyzickým jádrům, která zajišťují vyšší výkon v rámci multitaskingu (provádění více operací najednou). Minimálně 8 GB paměti RAM (Random Access Memory) pro rychlý běh aplikací, SSD (Solid-state drive) disk, který bude mít minimální paměťovou kapacitu 256 GB a bude zajišťovat rychlý start operačního systému včetně ukládání dat či programů. HD kameru pro online konference a porady. Značky Dell, Lenovo, HP a

Microsoft jsou nejvíce vhodné a prověřené řešení pro firemní klientelu již tím, že tuto kategorii notebooků vyvíjí mnoho let. K firemnímu notebooku by mělo být možné připojit dokovací stanici pro rozšíření stávajících konektorů a pro možnost připojení k externímu monitoru. Notebooky pro firemní klientelu by měly mít matný displej, především notebooky pro zaměstnance, kteří vykonávají svou činnost mimo kancelář. Měl by mít precizní zobrazovací schopnosti, které jsou definovány rozlišením a jasem displeje. Pro obchodníky jsou lepší kompaktnější modely do úhlopříčky 13 palců, s možností dotykového displeje pro snadnější prezentaci klientům a elektronické podepisování smluv na osobní schůzce. Dalším důležitým parametrem při výběrů notebooků pro kmenové zaměstnance bývá lehká bytelná konstrukce z hliníku a velmi dlouhá výdrž baterie. [32]

7.2 Workstation

Interním zaměstnancům, kteří pracují pouze v kanceláři, bývají přidělovány běžné stanice, z důvodů potřebného výkonu. Pokud firma vybírá z repasovaných zařízení, tak cenový rozdíl mezi desktopem a notebookem je zanedbatelný. U stolních PC je dobré se řídit podobnými pravidly jako u notebooků. Vybírat od renomovaných výrobců, kteří poskytnou co nejdelší záruku, a v případě problémů nabídnou On-Site servis (servis u zákazníka). Poté už záleží na žádaném výkonu.

7.3 Monitory, projektory

Pro administrativní pracovníky se často využívají monitory s možností nastavení výšky obrazovky a polohovatelným stojanem z pevného materiálu. Důležitým aspektem při výběru nových monitorů do firmy je typ jejich obrazovky. Matný panel, který nebude odrážet sluneční paprsky od oken, je optimální pro administrativní pracovníky, naopak lesklý displej je vhodnější pro grafické úpravy. Aktuálně nejvíce používaná technologie IPS (In-Plane Switching) zajišťuje kvalitní podání barev, které je přirozené pro oči. Má nízkou spotřebu a široké pozorovací úhly. Pozorovací úhly by měly dosahovat hodnoty okolo 180°. Full HD rozlišení má již v nabídce každý nový monitor a pro větší obrazovky je vhodné využít vyšší rozlišení až na úroveň 4K (Ultra HD). Nejvíce doporučované značky monitorů pro

firemní klientelu jsou Dell či HP. Nové moderní monitory již mají různé možnosti konektorové výbavy, včetně například napájení externího zařízení jako mobilní telefon. Základem je Display Port, nebo HDMI konektor (High-Definition Multimedia Interface) pro připojení notebooku či stolního počítače. [33]

7.4 Tiskárny a zobrazovací zařízení

Většina dokumentů se v moderní době uchovává elektronicky, přesto některou dokumentaci např. GDPR (General Data Protection Regulation) je nutné mít vždy i v papírové podobě. U tiskáren je nejdůležitější si předem určit, kolik lidí jí bude využívat a jaká je očekávaná vytíženost (počet požadovaných tisků stran za měsíc). S pořizovací cenou tiskárny také souvisí následný provoz. V případě, že si firma zakoupí multifunkční tiskárnu v hodnotě 1500 Kč, tak jedna inkoustová kazeta s výtěžností 100 stran bude stát 300 Kč [34], kde poté vychází tisk jedné strany na 3 Kč. Pokud by firma koupila tiskárnu za 27 tisíc Kč [35], následně ji bude stát inkoust s výtěžností 6.000 stran 380 Kč [36], což poté vychází jedna strana na 0,25 Kč (je nutno počítat 4krát, protože je každá primární barva zvlášť). Alternativním řešením je pořídit neoriginální náplně, což většinou bohužel bývá zdroj problémů, protože tiskárna si je schopná ověřit originalitu, a poté reportovat chybová hlášení, která nemají řešení. Návratnost takové investice nelze počítat prvotně na finance, ale na pohodlí a jistotu, že vše bude po dlouhou dobu funkční. Pokud si firma nemůže dovolit provést vstupní investici, jde zajistit alternativní řešení a vzít si tiskárnu na leasing, což dnes využívá mnoho společností. Uzavře se smlouva na minimální počet stran za měsíc a následně je firmě pouze fakturována předem domluvená částka za každou stranu (barevnou či černobílou). Nemusí se starat o údržbu ani doplňování spotřebního materiálu. Pokud cokoliv dochází, tiskárna automaticky pošle informací vlastníkově a do firmy je vždy zavčas dopraven nový spotřební materiál.

7.5 Periferie

Periferie jsou nezbytnou součástí kancelářského vybavení pro zaměstnance. Dokážou zajistit vyšší efektivitu a produktivitu práce. Pokud jsou pro zaměstnance

vybrány periferie od méně kvalitních značek, může se stát, že bude potřeba každé 2 měsíce měnit baterie. Možnou variantou je vyčlenit finance pro každého zaměstnance a nechat výběr periferií na něm samotném dle jeho potřeb a zvyků. Příkladnou specialitou jsou třeba vertikální myši. Ty lze zakoupit už od pár stokorun a splní potřebný účel eliminace nepřírozené polohy zápěstí a tím možný vznik zdravotních problémů.

7.6 Nábytek

Pracovní prostředí by mělo být různě modifikovatelné. Optimálním řešením jsou polohovatelné stoly, tzv. ergonomické, které lze vertikálně posouvat a zajišťovat pohodlí pro všechny typy lidí dle jejich tělesných dispozic. Pracovní deska by měla mít dostatečný prostor, aby se na ní mohl umístit monitor a zároveň zbylo dost prostoru pro práci s papírovými dokumenty.

Pracovní židle/křeslo je taktéž maximálně důležitým pracovním nástrojem. Na židli člověk sedí celé hodiny a pracuje v určité často fixované poloze. Křeslo by mělo mít kromě vertikálního posouvání také polohování opěrky. Nastavení hlavové opěrky do potřebné výšky, nastavení loketních opěrek do potřebné výšky a také do stran. Příjemným benefitem je posunutí bederní opěrky dle fyziologických potřeb dané osoby. [37]

7.7 Konferenční místnosti

Vybavení konferenčních místností by mělo být v souladu s patřičným komfortem pro účastníky konferenčního jednání, či školení. Dobře osvětlená místnost přirozeným světlem z venkovního prostředí, která může být v případě potřeby zregulována až na úroveň úplné tmy a následného využití LED osvětlení pro meetingy v pozdních hodinách. V případě, že v nemovitosti není ideální přísun přirozeného světla, je možné využít specializované technologie světlovodů, které dokážou dopravit do nemovitosti chybějící přirozené světlo. Pro konferenční prostory je na zvážení, využít klimatizační jednotky s čističkou vzduchu. Prioritním zařízením je kvalitní projektor s vhodnou lampou dle svítivosti. Součástí projektoru by mělo být delší vedení kabeláže až ke konferenčnímu stolu s určitou

rezervou, aby se mohlo promítat z jakéhokoliv zařízení. Je třeba zajistit rozsáhlou konektorovou výbavu. Konektor VGA, HDMI, USB-C, Lightning, potřebné redukce a bezdrátové spojení pro sdílení obrazovky. Případnou alternativou pro promítání by mohlo být využití větší televize. Ozvučení místnosti je velice zásadní. Místnost by měla splňovat požadavky na akustiku tak, aby byl přednášející zřetelně slyšen, a audio ozvučení pro komfortní poslech prezentace po celé místnosti.

V případě, že bude nutné zasedací místnost využívat i ke konferenčním hovorům, je dobré ji vybavit kvalitními mikrofony a kamerou s vysokým rozlišením.

V rámci nábytku zvolit především křesílka pro pohodlné sezení. Za součást konferenční místnosti lze automaticky považovat nějaký flipchart nebo tabuli s dostatkem psacích potřeb. Příjemným bonusem může být automatický kávovar, menší tiskárna či lednička.

Microsoft má přímo připravené tzv. autonomní zařízení, viz například Microsoft Surface Hub 2S, které je po zakoupení umístěno v konferenční místnosti, přihlášeno do cloudu a může se k němu připojit jakýkoliv účastník konference. [38]

8 Softwarové vybavení firmy

Za software se dá považovat jakýkoliv program či aplikace. Software je definován jako přesný opak pojmu hardware. Software je ta součást IT, na kterou si nelze sáhnout, jelikož není hmatatelná. Mezi software se dá například zařadit jakýkoliv grafický program, operační systém, počítačová hra, kancelářská aplikace, firmware (software, který je od výroby nahrán do hardwarového zařízení – typicky BIOS, řídicí software). Softwarem je i škodlivý kód v různých podobách počítačového viru.

Většina softwaru je placená, přestože se často najdou alternativy v oblasti freewaru (volně dostupný software), ale ty jsou určeny spíše pro domácí použití. Je možné zmínit variantu open-source, což je software, který má otevřený kód (např. operační systém Linux či Android) a každý uživatel si jej může upravit dle svých potřeb. Ve firemní sféře budou zákazníci odkázáni na placený software, který bude

opatřen licencí pro použití v podnikání, zato několikanásobně dražší než pro domácí použití. Lze uvést operační systém Windows 10 Home pro domácnosti, kterému na rozdíl od Windows 10 Pro chybí komponenty pro připojení do domény, nástroje pro správu a další funkce určené pro firemní využití. V případě softwarového produktu Office se dá zakoupit domácí verze, nicméně proto, aby byla splněna licenční ujednání pro firemní využití, bude třeba zakoupit jinou, zřejmě dražší licenci, přestože se funkcionalitami příliš neodlišuje. Nákup licencovaného softwaru se netýká pouze počítačů, ale mnohokrát se může stát, že licenční ujednání bude opravdu striktní. Proto v případě Office 365, který je pro mobilní zařízení zdarma, bude třeba u zařízení stylu iPad Pro zakoupit pro uživatele plnou licenci, protože dle společnosti Microsoft, zařízení s obrazovkou větší jak 10,1“ není mobilní zařízení. [39] U softwarových produktů se lze setkat s 2 typy licencí. Doživotní licence a licence typu subscription, které jsou jako SaaS (Software as a Service). Například u Windows Serveru a jejich podružných CAL licencí (Client Access Licenses) je často nutné najmout specialistu na licence, který se o tuto problematiku postará.

8.1 Office 365 -> Microsoft 365

Dříve se jmenoval tento produkt/služba Office 365, od poloviny roku 2020 se již označuje jako Microsoft 365. Byl poprvé vydán v roce 2011 a od té doby byl již několikrát updatován. Tento produkt byl primárně určen pro firemní klientelu, dnes je běžnou součástí každého koncového uživatele, díky jeho zcela jednoduchému a pohodlnému užívání.

Jak bylo definováno, Microsoft 365 se dá používat pouze jako SaaS. Aktuálně (jaro 2022) jsou jen 3 licence, a to Microsoft 365 Business Basic za 5 USD, Microsoft 365 Business Standard za 12,5 USD a Microsoft 365 Business Premium za 20 USD. [40]

Velkým benefitem této služby je možnost sdílení v rámci více zařízení. Funkcionalita, kdy v jeden moment má k programu Word přístup vícero uživatelů, je dokonalý pracovní nástroj. Uživatelé se mohou podílet na jednom projektu, u toho být v konferenci pomocí Microsoft Teams a využívat aktivního

brainstormingu. To samé řešení u aplikace Excel, PowerPoint je obdobné a zcela bezkonkurenční. Studenti či kolegové, kteří pracují na jednom projektu, získají z této funkcionality opravdu maximum a práce na daném projektu bude efektivnější. Výhodou v rámci firemního cashflow je měsíční platba pouze za uživatele, kteří službu aktivně využívají. Všechna data jsou v maximálním bezpečí díky tomu, že jsou provozována na serverech vlastněných společnostmi Microsoft. Další výhodou je úspora dat na lokálním disku, jelikož není třeba žádných instalací. S tím souvisí i výkonnost daného zařízení, které není zahlceno mnoha aplikacemi. Není nutné produkty ručně aktualizovat, vždy jsou plně aktualizované a není potřebné se o cokoliv starat – pouze platit.

Dle náznaků posledních let je zřejmé, že doba standardně licencovaných produktů již dávno pominula tím, že se vše přesouvá do cloudu. Přestože jsou tyto produkty celého balíku Microsoft 365 provozovány v cloudu, jsou přístupné i v případě ztráty síťové konektivity. Jistým benefitem je využití Office 365 z jakéhokoliv typu zařízení. Telefon, tablet, či notebook.

Provoz všech cloudových služeb skrývá i svou negativní stránku věci a Microsoft ji zcela jistě předpokládal a využil. Jedná se o možné zdražení služeb, což je jedna z mála nevýhod cloudových řešení. Microsoft a další firmy rády svými službami lákají na cloud, protože je tento typ licence ve většině případů ekonomicky výhodnější pro pružné společnosti. Riziko nastává až v situaci, kdy firma již plně funguje v cloudu. V tu chvíli může přijít zdražení této služby a uživatelé (firmy) se musí podřídit, přestože se zdražením nesouhlasí, jelikož služby s tímto produktem potřebují.

8.2 Adobe

Společnost Adobe již mnoho let vyvíjí a vylepšuje kancelářský balík pro práci s PDF soubory. Pokud je nutné soubory jen otevírat a tisknout, stačí pouze webový prohlížeč. Většina z nich má možnost čtení PDF souborů integrovanou v sobě. Pokud je ale potřeba dokumenty tvořit na hlubší úrovni, upravovat, vytvářet interaktivní dokumenty a digitálně je podepisovat, je potřebné sáhnout po specializované aplikaci, která bude s největší pravděpodobností placená. Nejpoužívanější je aplikace od společnosti Adobe, která již také přešla na podobu

SaaS, takže zákazník měsíčně platí a oni dodávají software. Aktuálně (jaro 2022) požadují něco málo přes 500 Kč za jednu licenci. [41] Součástí licence je i malý cloudový prostor, který však díky Microsoft 365 není třeba využívat. Také je k dispozici multiplatformní desktopová aplikace a aplikace pro mobilní zařízení. Adobe si zakládá na svém výborném OCR (optické rozpoznávání znaků), který umí i český jazyk. Ve chvíli, kdy je naskenován dokument, Acrobat ho sám rozpozná, zpracuje a je možné ho poté i upravovat. Dají se vyplňovat dokumenty k tomu určené, i ty, které na to nejsou připravené, a hlavně požádat kohokoliv o digitální podpis.

Adobe není jen aplikace Adobe Acrobat, ale zabývá se primárně grafickými programy. Opět jako u Acrobatu je platba prováděna měsíčně, a to buď necelých 800 Kč za jednu aplikaci dle výběru, nebo 1800 Kč za všechny aplikace. [42] Záleží, co zaměstnanci potřebují ke své práci a jestli aplikace dokážou využít.

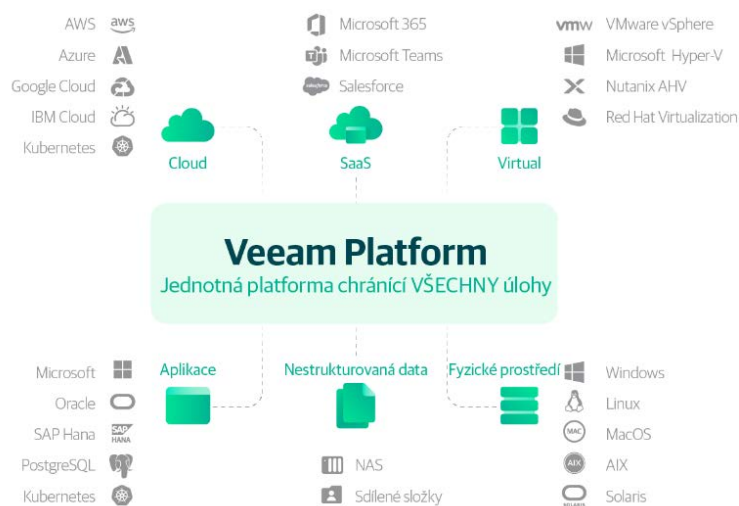
Ty nejpoužívanější jsou Adobe Sign, sloužící pro plně digitální podepisování dokumentů, Adobe Photoshop pro pokročilou práci s grafikou, profesionální úpravu fotografií, vytváření grafických návrhů, vizitek a mnoho dalšího. Jeho podstatnou výhodou je práce s vícero grafickými vrstvami a díky tomu širokými možnostmi, jak daný grafický návrh upravovat, i když na něm již bylo aplikováno mnoho dalších úprav. Adobe Lightroom by se dal považovat za zjednodušený Adobe Photoshop. Primárně je využíván pro práci s fotografiemi. Adobe Premiere je jako profesionální program využíván pro úpravu a střih videa, Adobe After Effects zajistí dokonalé video efekty, přechody při vytváření kratších filmů a vytvoření titulků. Dále se v balíku Adobe Creative vyskytuje program Adobe Dreamweaver, Adobe Illustrator a další.

Celkovým pohledem na balík Adobe (cloudová služba Adobe Creative Cloud) lze definovat jako dokonalé spojení vícero programů (v rámci jednoho online prostředí), které spolu navzájem skvěle komunikují a spolupracují na požadovaných projektech. Možnou nevýhodou může být použití aplikace s jednou licencí pouze na 2 zařízeních najednou. Pokud ji chce uživatel spustit na třetím zařízení, je nutné se z předešlého odhlásit.

8.3 Zálohy

Benefitem cloudového řešení mohou být automatické zálohy. IT správce se tak nemusí o zálohování moc starat a má je předplacené licencí. Všechna důležitá data jsou uložena na serveru poskytovatele služby. Daný poskytovatel se kompletně postará o bezpečnost dat a jejich zálohování. Na zálohy operačního systému lze zmínit známou společnost Veeam a jejich produkt určený pro firemní sféru Veeam Backup&Replication.

V zálohování není žádné omezení. Za řešením Veeam je dlouholetý vývoj, který zaručuje kvalitní produkt. Služba ideálně kombinuje výkon, jednoduché použití a cenovou dostupnost. Hlavní podporovanou funkcí je automatizované testování záloh a velmi rychlé obnovení. [43] Na obrázku (viz Obrázek 7) lze vidět, které všechny platformy společnost Veeam podporuje.



Obrázek 7 Veeam Platform, zdroj: [44]

Z pohledu hardwaru a zálohování je důležité nejen zálohování dat, ale zařízení jako takových. Nemělo by se opomenout využívání záložních zdrojů energie. Nejznámějším je typ UPS (Uninterruptible Power Supply), který zajistí zálohu na lokálních serverech či lokální síťové infrastruktuře. Většinou pouze zabezpečí energii po dobu nezbytně nutnou k řádnému uložení dat a následnému bezpečnému vypnutí zařízení, než opět dojde k obnově dodávek z veřejné sítě.

8.4 Operační systémy (OS)

Jedná se o hlavní software počítače či serveru, díky kterému lze používat jakékoliv další softwarové produkty nebo služby. Operační systém také zajišťuje komunikaci mezi počítačem a jeho uživatelem. Může být také nazván rozhraním. Díky OS může být celý systém rozšířen o další programové funkce a uživatelé mohou využívat jeho potenciál. Ve firemní sféře lze pro běh určitých aplikací využít open-source operační systém Linux, přesto jsou zde popsány pouze licencované OS vyvinuté společností Microsoft. Operační systém lze zakoupit ve dvou provedeních, a to buď v FPP (Full Package Product) verzi či OEM verzi. Tyto 2 varianty mají své výhody i nevýhody použití. Výhodou FPP verze je její plná přenositelnost. Je možné ji nainstalovat na jakýkoliv počítač a také ji použít opakovaně v případě výměny daného zařízení za jiné. Naopak OEM verze je levnější, má ale určitá omezení. Je vázaná na konkrétní zařízení, na konkrétní základní desku a nelze ji tak instalovat na jiné zařízení. Oba typy licencí OS lze libovolně upgradovat na novější verzi. [45]

Operační systémy ve firemní struktuře lze rozdělit na 2 typy dle využití. Rozlišují se operační systémy pro PC a notebooky, které využívají zaměstnanci a operační systémy pro IT infrastrukturu. Jako OS pro zaměstnance se většinou využívají ty nejnovější, případně se vždy upgradují na nejnovější verzi. Aktuálně (jaro 2022) je nejnovější systém od společnosti Microsoft, konkrétně Windows 11 Pro. Pro firemní klientelu se výhradně využívají produkty s dovětkem „Pro“.

Porovnáním verze Home a Pro [46] lze zaznamenat, že jsou si velmi podobné. Verze Pro má navíc bezpečnostní funkci. Pokud dojde ke ztrátě nebo krádeži počítače, produkt BitLocker celé zařízení uzamkne a nikdo další nezíská přístup do systémů a jejich dat. Obsahuje také několik dalších funkcí a výhod, které se ve firemní sféře hodí. Systém ve verzi Pro lze provázat s Active Directory a zajišťuje vyšší bezpečnost dat. Propojením Windows 11 Pro a Windows Server se dají spravovat počítače, uživatelské účty a skupiny. Snadno se tím uživatel dostane ke sdíleným souborům a tiskárnám a celkově dochází k zjednodušení základních funkcí a rozšíření o funkce, které napomohou efektivnější komunikaci ve firemní síti. Pro servery je nejčastěji využíván OS Windows Server, aktuálně Windows Server 2022. Jedná se o OS přizpůsobený službám a potřebám serveru. Je zde důraz na vyšší bezpečnost a spouštějí se na něm náročnější aplikace. Také se klade

důraz na flexibilitu a dostupnost. OS Windows Server je propojitelný se službou Azure a má tři edice. Edici Standard, Essentials a Datacenter. Každá edice se hodí pro jiný typ firmy dle počtu zařízení, potřeb virtualizace, SDN atd. [47]

8.5 Licenční politika

Licencování produktů prošlo velkou obměnou, hlavně u společnosti Microsoft. Každá firma má možnost zvolit si licenci dle jejich požadavků tak, aby odpovídala všem potřebám.

FPP licence a licence typu OEM byly popsány v podkapitole 8.4. Dále se dají využít různé multilicenční produkty, které jsou určeny pro firmy, co potřebují licencovat daný produkt pro mnoho svých zařízení. Aktuálně vzhledem k přesunu celého světa do cloudu se využívají především produkty s licenci typu SaaS. [48] Produkt je firmě pronajímán, dokud za něj platí měsíční poplatky. Dá se tak měsíčně zakoupit licence pro používání dané služby, či aplikace pro určitý počet uživatelů a díky tomu se dá výrazně ušetřit. Nevýhodou je zmiňovaná nízká kontrola nad produktem. Firma je na tomto produktu více závislá a v určitých případech to nemusí být žádoucí. Některé firmy chtějí být maximálně nezávislé a více jim vyhovuje produkt přímo vlastnit než ho mít v pronájmu. SaaS je extrémně výhodný v rámci úspory času a nasazení pro celou firemní infrastrukturu pro daného IT správce. Pro použití programů licencovaných pomocí SaaS stačí internet a prohlížeč, ve kterém jej spustí. Firmě to vypomůže v jejich startu, jelikož počáteční náklady na pořízení a využívání takových služeb jsou velmi nízké. Zaměstnanci vidí benefity ve vysoké dostupnosti a automatických zálohách souborů, bez obav ze ztráty dat.

8.6 Podnikový informační systém

„ERP systém je komplexní informační systém, který je v dnešním moderním světě pro mnoho společností centrálním mozkiem firmy. Systém soustřeďuje a zná klíčové detaily a data podniku počínaje od účetnictví, které je součástí každého ERP systému a u jednoduchých modelů je jedinou oblastí v ERP systému zpracovávanou, přes zpracovávání podnikových procesů od správy dodavatelské a odběratelské sítě, přes

objednávkový systém, plánování kapacit až po složitější procesy, jakým je například plánování výroby a její řízení. Pro pokrytí co největšího množství podnikových procesů je důležitá také integrace ERP systému s jinými softwary.“ Převzato z [49]

Výhodou využití ERP (Enterprise Resource Planning) systémů je jejich flexibilita (mobilita). Procesy a přístupy se dají řídit pomocí počítače či chytrého telefonu. Typickým rysem ERP systémů je automatizace většiny procesů, kdy systém zvládne automatizovaně zasílat emaily, zakládat faktury, či pracovat s přijatými soubory dle předem specifikovaných definic. Díky ERP systémům lze jednodušeji pracovat s velkým množstvím dat uložených v databázi, sledovat cashflow, kontrolovat specifické procesy ve firmě a potlačovat lidskou chybovost.

Většina podniků má ERP systém propojený právě s CRM (Customer Relationship Management) systémem, který pomáhá zajišťovat komplexní přehled nad zákazníky dané firmy, pracuje s kompletní databází kontaktů a lze k nim přistupovat pod určitými rolemi.

Příklady podnikových informačních systémů: Helios, SAP, Oracle, Microsoft Dynamics. Podnikový informační systém v sobě dále může integrovat další informační systémy jako:

SCM – Supply Chain Management – obstarávající dodavatelský řetězec.

APS – Advanced Planning and Scheduling – pro pokročilé plánování a opět řízení dodavatelského řetězce, mnohdy bývá součástí zmíněného ERP.

HRM – Human Resource Management – starající se o řízení lidských zdrojů, obvykle spadá pod kompetence personálního oddělení, kde slouží k utváření záznamů a analýzám náborů, školení nebo jiného vzdělávání zaměstnanců.

MIS – Management Information System – sloužící k operativnímu a taktickému rozhodování a řídicím procesům v oblasti nákupu či prodeje, jedná se o nadstavbu ERP.

EAM – Enterprise Asset Management – ke správě podnikových zdrojů nebo správě životního cyklu zařízení, která může snižovat náklady na údržbu a obnovu strojů.

DMS – Document Management System – zastřešující veškerou manipulaci s elektronickými dokumenty a jejich obsahem.

BPM – Business Process Management – pro znázornění a realizaci podnikových procesů v kontextu okolí, stará se o optimální průběh procesů a efektivní rozvržení času, souvisí tak se zvýšením konkurenceschopnosti podniku.

BI – Business Intelligence – ke statistickým a analytickým výpočtům, práce s big data, propojení různých datových zdrojů. Převzato z [50]

9 Koncept vlastní implementace

V navazující, praktické části, této bakalářské práce se lze detailně podívat na implementaci vlastního řešení. Prvotně budou shrnuty výsledky dotazníku [51], který byl vytvořen a rozeslán mezi osoby, které mají, co dočinění s IT, ať jako studenti, učitelé, grafici, vývojáři či přímo IT specialisti za účelem průzkumu veřejného mínění a pro prokázání znalostí v oboru. Dotazník posloužil jako inspirace a další pomocný materiál při tvorbě návrhu vlastního řešení. Tento dotazník byl vytvořen za pomoci cloudové služby, konkrétně Microsoft Forms, která je jedním z programů online balíku Microsoft 365.

První dotaz směřuje na cloudové služby. Požadavkem bylo vybrat z možných variant, které cloudové služby pro podniky jsou pro ně známé. K výběru byl Kerio Connect (alternativní poštovní server), Email Profi od Seznamu, Office 365, Amazon WorkMail, Google Workspace (kalendář, pošta a sdílení dokumentů v prostředí od společnosti Google) nebo bylo možné zvolit něco jiného, co dotyční znají a dopsat jej do zvoleného pole. Dalším dotazem bylo vybrat z nabídky síťových prvků, které by se daly definovat jako SDN a o kterých již slyšeli. Z variant k výběru bylo: UniFi Network, MikroTik, Aruba Instant-ON, Cisco Meraki, FortiNet. Případně opět bylo možné zvolit něco jiného, co respondenti znají. Jednou z uzavřených otázek bylo odpovědět ANO/NE na otázku „Pokud bys zakládal společnost, volil bys z možnosti moderního IT?“ Pod pojmem „moderní IT“ bylo myšleno využití cloudových služeb. Na tuto otázku navazovala další „Které z cloudových řešení by sis vybral, pokud bys zakládal společnost?“ Na výběr bylo z variant: Google Workspace, Email Profi od Seznamu, MailServer poskytovaný tvým dodavatelem webhostingu, Amazon WorkMail, Office 365, KerioConnect či zvolit

vlastní odpověď. Poslední dotaz byl směřován na výrobce. Respondent měl zvolit výrobce síťových prvků, kterého by zvolil pro svou vlastní implementaci. Na výběr bylo z variant: UniFi Network, MikroTik, FortiNet, Aruba Instant-ON, Cisco Meraki. Závěrem bylo nutné uvést, v jakém postavení se respondent právě nachází. Zda-li jako student, případně jakého oboru a stupně, či ročníku studia, učitel, IT specialista nebo jiná pozice.

9.1 Výsledky dotazníku

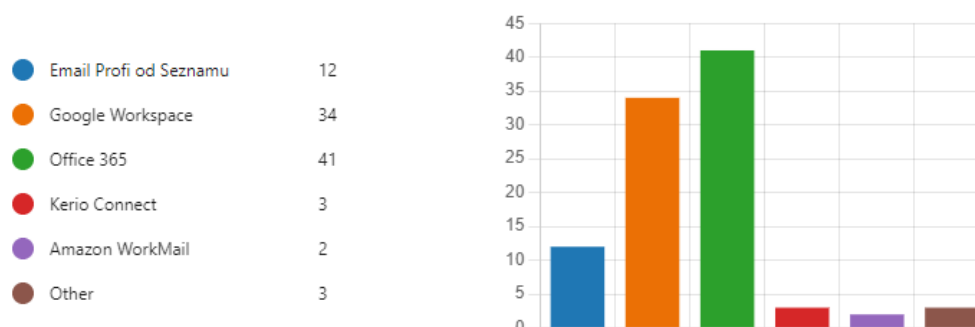
Na tento dotazník bylo získáno celkem 42 odpovědí především od lidí, kteří tyto pojmy alespoň nějakým způsobem znají. Byli osloveni bývalí studenti ze Střední školy aplikované kybernetiky, stávající studenti z Univerzity Hradec Králové a pár lidí přímo z oboru IT.

Vyhodnocení dotazníku proběhlo automaticky za pomoci vybraného programu a z přehledných grafů lze vyvodit, že nejvíce lidí zná cloudové řešení od společnosti Microsoft, konkrétně Office 365/Microsoft 365 a Google Workspace. Ohledně síťových řešení znají v Česku nejrozšířenější MikroTik a pro vlastní implementaci zcela jasně převažuje Office 365/Microsoft 365 jako moderní cloudové řešení. Přestože většina zná společnost MikroTik, pro vlastní implementaci by zvolila Cisco Meraki nebo UniFi Networks.

Z cloudových služeb (viz Obrázek 8), znají Office 365, dále Google Workspace a na třetím místě Email Profi od Seznamu. Zbylé cloudové služby téměř nikdo neznal.

1. Které cloudové služby pro podniky znáš

[More Details](#)

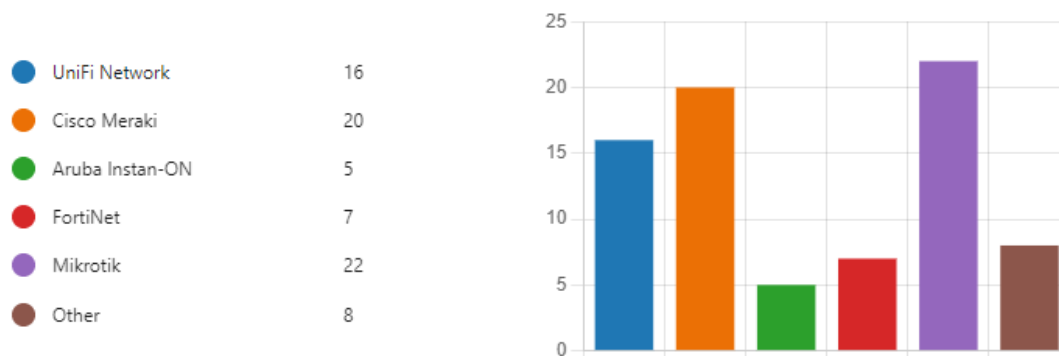


Obrázek 8 Výsledky dotazníků, zdroj vlastní zpracování

Z odpovědí na otázku (viz Obrázek 9) vyplynulo, že lidé nejvíce znají síťové prvky MikroTik, dále Cisco Meraki a také UniFi Networks. Ostatní zná méně než 8 respondentů.

2. Které řešení síťových prvků které by se dali definovat jako SDN znáš?

[More Details](#)

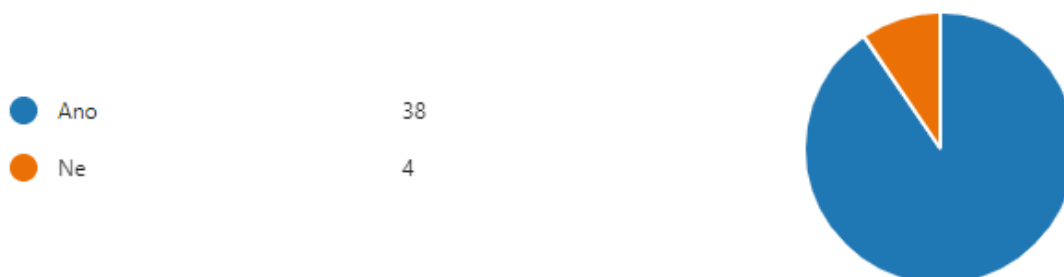


Obrázek 9 Výsledky dotazníku, zdroj vlastní zpracování

Velmi zajímavým faktem na uzavřenou otázku číslo 3 (viz Obrázek 10) ohledně toho, zda by respondent volil moderní řešení při zakládání nové firmy a potřeby IT řešení, tak téměř všichni odpověděli, že ano.

3. Pokud by jsi zakládal společnost, volil by jsi z možnosti moderního IT?

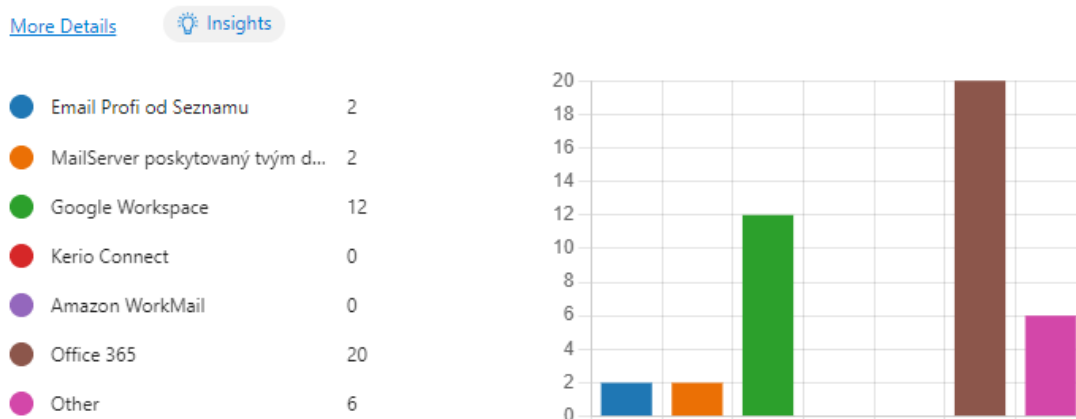
[More Details](#)



Obrázek 10 Výsledky dotazníku, zdroj vlastní zpracování

Navazující otázka číslo 4 (viz Obrázek 11), pokud by volili moderní řešení založené na cloudové službě, ukázala dle odpovědí, že by nejvíce využili cloudovou službu Office 365 a Google Workspace. Taktéž by pár respondentů využilo jiné individuální řešení.

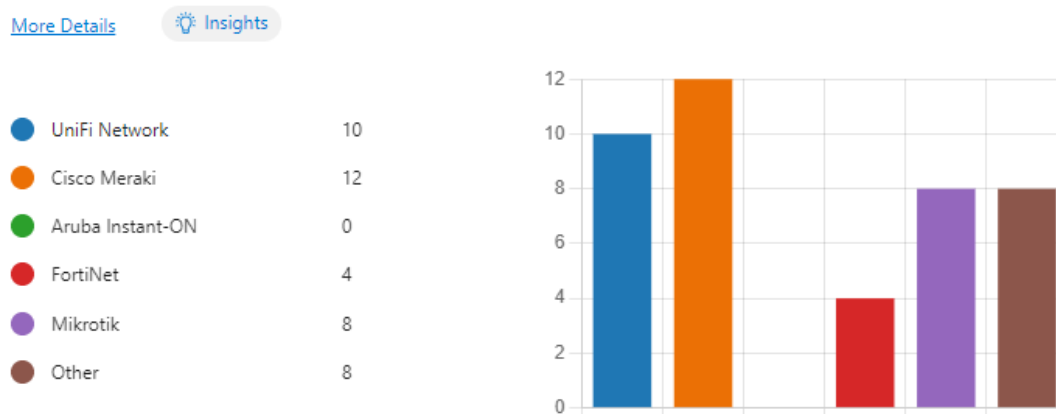
4. Které z cloudových řešení by sis vybral, pokud by jsi zakládal společnost?



Obrázek 11 Výsledky dotazníku, zdroj vlastní zpracování

V oblasti síťových prvků respondenti nejvíce znají firmu Cisco, která je nejvíce známá a její portfolio již zaznamenal každý správce IT. Většina respondentů (viz Obrázek 12) by zvolila řešení právě od této firmy a konkrétně Cisco Meraki. Jako případná alternativa se těsně umístila velmi známá společnost UniFi Networks a jako třetí v pořadí skončily prvky od Lotyšské firmy MikroTik. Někteří by dokonce zvolili úplně jiné řešení.

5. Kterého výrobce síťových prvků by jsi vybral?



Obrázek 12 Výsledky dotazníku, zdroj vlastní zpracování

21 respondentů ze 42 jsou studenti vysoké školy a 2/3 z nich studují bakalářský obor. Zároveň 18 respondentů z 22 studují technický obor, tudíž mají k tématu co říct. Zbylí respondenti pracují v oboru a jsou na pozici IT specialisty, vývojáře, grafika, či jiném. Graficky znázorněno níže (viz Obrázek 13 a Obrázek 14).

6. Jsi student?

[More Details](#)

 Insights

● Střední škola	1
● Vyšší odborná	0
● Vysoká škola	21
● Ne	20



7. Jaký stupeň vysoké školy studuješ

[More Details](#)

● Bakalářský	13
● Magisterský	7
● Doktorský	1



8. Studuješ některý z technických oborů?

[More Details](#)

 Insights

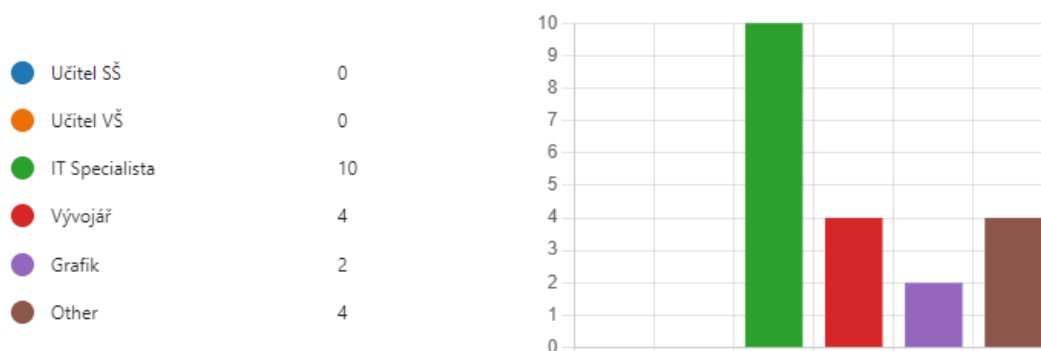
● Ano	18
● Ne	4



Obrázek 13 Výsledky dotazníku, zdroj vlastní zpracování

11. Jaká je tvá pozice?

[More Details](#)



Obrázek 14 Výsledky dotazníku, zdroj vlastní zpracování

9.2 Vlastní návrh řešení

Vlastní návrh řešení vychází z nasbíraných vědomostí při studiu na Střední škole aplikované kybernetiky v Hradci Králové se zaměřením na Počítačové sítě. Zde bylo možné absolvovat projekty, které přímo souvisely s oborem IT. Při jednom z projektů, se podařilo optimalizovat pokrytí školicího střediska technologií WiFi, ve velmi nevhodné lokalitě vzhledem k zrušení a použití nevhodného stavebního materiálů obvodových i vnitřních zdí. Další vědomosti z IT oboru byly nasbírané při studiu na fakultě informatiky a managementu (Univerzita Hradec Králové).

Zkušenosti z oblasti managementu a lidských zdrojů použité v této části práce vycházejí z osobního pozorování, častého dotazování a komunikací se zaměstnanci a majiteli firem. Dále z osobního studia výkonných manažerů na vedoucích pozicích a jejich pracovních aktivit.

9.2.1 Analýza požadavků a potřeb firmy

Než se zrealizuje jakékoliv řešení, měla by se provést vstupní analýza potřeb a požadavků konkrétní firmy, na kterou má být řešení implementováno. Analýza může mít více podob a být přímo definovaná pro určitou oblast následné implementace nebo být více obecná v rámci prostého dotazování se nad celou problematikou, která byla použita zde. Řešení by mělo být vždy individuální a vycházející z odpovědí na požadavky aktuální i budoucí. Níže je zmíněno pár otázek, na které by se měl realizátor zeptat před navrhováním možných řešení.

Plánujete si pronajmout komerční prostor nebo chcete prostory nové pobočky dlouhodobě vlastnit? V jakém stavu se aktuálně jednotka nachází? (Kabeláž, prostory, dispozice)

Jaké množství financí máte možnost investovat do IT ve Vaší firmě?

Chcete ve firmě využívat chytré řízení a automatizaci?

Jakým způsobem budete řešit fakturaci a účetnictví? Chcete mít vlastní databázový systém, nebo využívat hostovaný?

Chcete vlastnit softwarové produkty a spravovat je na vlastním HW zařízení?

Chcete mít doživotní licence, nebo preferujete plně aktuální aplikace?

Jak chcete řešit bezpečnost? Je pro Vás důležité mít data uložena lokálně? Jak přemýšlíte nad ztrátou důležitých dat? Co by to pro Vás znamenalo?

Kolik Vás stojí 1 hodina provozu zastavené firmy, kvůli výpadku?

Máte časové možnosti k tomu teď tvořit velký projekt a připravovat infrastrukturu, nebo chcete mít HW a SW služby rychle zavedené? Chcete využít výhod virtualizace?

Jak rychlé internetové připojení potřebujete pro svou činnost?

Potřebujete mít zajištěnou online konektivitu 24/7? Budete využívat pouze bezdrátové spojení pro pokrytí pobočky nebo požadujete v každé místnosti internetovou zásuvku napojenou až do patch panelu, který je propojen se switchem, umístěným v racku?

Kolik bude na pobočce stálých zaměstnanců a jakou budou vykonávat činnost?

Kolik pracovníků bude potřebovat využívat cloudové služby jako Microsoft 365, Adobe Creative Cloud?

Budou zaměstnanci využívat své vlastní notebooky, nebo pouze firemní?

Jak si představujete sdílení dat a dokumentů v rámci firmy?

Kterou aplikaci chcete využívat pro komunikaci ve firmě?

Budete potřebovat často tisknout fyzickou dokumentaci? Kolik stránek měsíčně bude třeba tisknout? Barevně, či černobíle? (zdroj: vlastní zpracování)

Zavedení nové pobočky prošlo stejnou, výše popsanou analýzou, ze které vyplynulo, že tato investiční společnost chce využívat především cloudové řešení založené na licencích subscription a nechce vlastnit své vlastní servery kromě menšího NAS.

9.2.2 Porovnání a výběr síťových prvků Cisco Meraki vs. UniFi Networks

Pro realizaci nové pobočky se muselo udělat rozhodnutí o nákupu síťových prvků. Bylo důležité zvolit, na jaké platformě bude celá síť postavená. Konečné rozhodnutí se udělalo po pročtení několika internetových článků [52], vyhodnocení dotazníkového průzkumu a po načerpání informací na internetových fórech. Mezi finální výběr se zařadila společnost Cisco se svojí produktovou řadou Meraki a společnost Ubiquiti se svou produktovou řadou UniFi. Tato dvě řešení ve výsledku nejlépe odpovídala požadavkům firmy a preferenci IT administrátora vycházející z historických zkušeností.

Licencování produktů Cisco není zcela jednoduché na pochopení. Bez zaplacení předplatného tyto produkty nebudou funkční a licence jsou drahé. Je možné získat zvýhodněnou cenu, ale je třeba si tyto licence předplatit na mnoho let dopředu. Pro to, aby IT administrátor správně nakonfiguroval síťové prvky většinou, musí absolvovat speciální školení přímo od firmy Cisco. Produkty této značky jsou velice uzavřené a není možné do jejich systému zasahovat a přizpůsobovat více, než je povoleno. Technická podpora je pouze za příplatek. Kromě všech zmiňovaných vlastností jsou tato řešení výrazně dražší oproti UBNT.

U společnosti Ubiquiti je mnoho věcí naopak. Cena prvků je velmi přívětivá oproti Meraki. Technická podpora je bezplatná a součástí každého produktu, zároveň pro tyto prvky existuje komunita, která si navzájem radí a pomáhá. Konfigurace těchto prvků je velmi jednoduchá a uživatelské rozhraní je taktéž velmi přívětivé. Prvky Ubiquiti nemají žádnou licenci, kterou by si zákazník musel předplácet. Všechny funkce, které tyto prvky mají, jsou v ceně. Přestože je podpora zdarma, občas si zákazníci stěžují, že je nedostatečná. Nicméně mají k dispozici zmiňovaná fóra, kde mohou o svých problémech diskutovat a najít řešení. Prvky UniFi nemají žádnou vlastní baterii a ke svému provozu vždy potřebují externí zdroj napájení – všechny modely mají PoE. Konfigurace prvků probíhá přes jeden centrální bod, který funguje v cloudu. Toto síťové řešení zvládne nakonfigurovat i méně zdatný IT technik, nepotřebuje speciální školení jako u prvků Cisco. AP UniFi nabízí 360 ° pokrytí WiFi signálem.

Porovnáním se zjistilo, že ačkoliv produkty od společnosti Cisco mají mnoho funkcionalit navíc, tak prvky Ubiquiti jsou daleko jednodušší na konfiguraci a celkovou správu. [53] Vzhledem k provedené analýze potřeb se došlo k závěru, že vhodnější bude nasadit prvky od společnosti Ubiquiti vzhledem k potřebě vytvořit relativně malou síť, kterou chce IT správce jednoduše konfigurovat a nejsou potřeba pokročilé funkce.

9.2.3 Porovnání a výběr řešení On-premise vs. Cloud

Jak již bylo zmíněno, při řešení „On-premise“ je software instalován lokálně, naopak u cloudového řešení firma nemusí řešit svůj vlastní server, kde bude mít lokálně instalovaný software, ale využívá cizího hardwaru a jen užívá licenci typu subscription, kdy měsíčně platí za počet uživatelů a za balík aplikací, či jednotlivých aplikací/služeb.

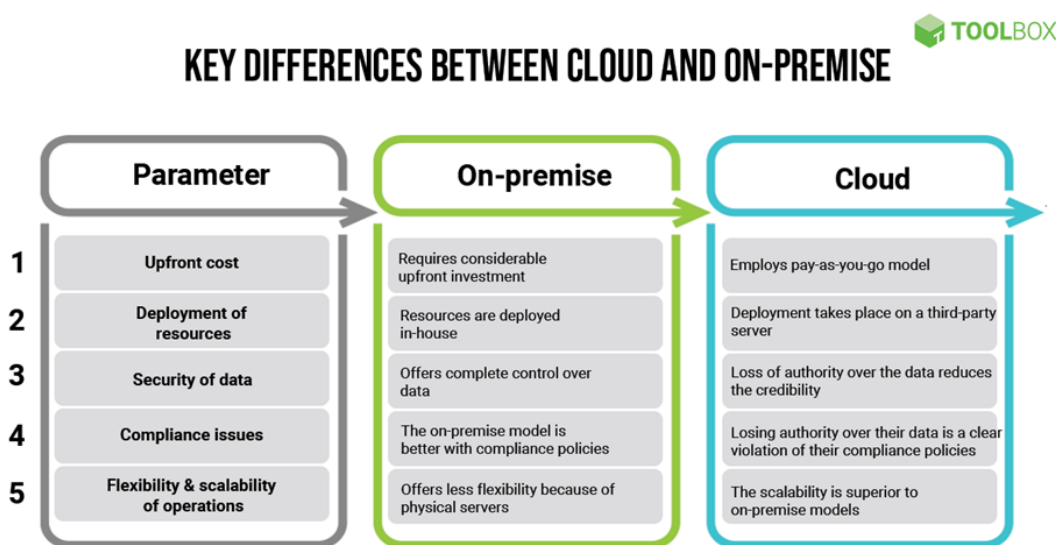
Při porovnání dvou možností, jak řešit služby pro středně velkou firmu bylo zjištěno (viz Obrázek 15), že je třeba prvně zohlednit finanční náročnost. U cloudového řešení se neplatí žádná vstupní investice, u varianty On-premise je to naopak a vstupní investice jsou vysoké. Je důležité zmínit, že se nejedná pouze o vstupní investice, které je třeba započítat. Firmou využívané produkty a služby se v čase mění, aktualizují a modernizují. To v případě Cloudu na základě měsíčního poplatku řeší dodavatel. U On-premise řešení si aktualizace obstarává klient a pokud chce mít celé portfolio stále aktuální, stojí ho to nemálo času a financí nejen za software, ale i obnovu hardwaru.

Rychlost zavedení těchto služeb hraje důležitou roli při startu firmy a při jejím růstu. Cloudové řešení se dá zavést velmi rychle, u On-premise řešení to je časově náročnější proces.

Při pohledu na bezpečnost lze zjistit, že u řešení On-premise se o systémovou bezpečnost kompletně stará zákazník a přebírá za ní plnou zodpovědnost a kontrolu. U cloudu se o systémovou bezpečnost stará firma, která tuto službu poskytuje, nicméně je třeba dbát na správcovské účty a oprávnění k datům. Mnoho zákazníků se může o svá citlivá data bát, ale opak je zde pravdou. Obrovské společnosti poskytující cloudový způsob přístupu k aplikacím, mají díky velkému finančnímu kapitálu, bezpečnost velmi dobře zvládnutou.

Důležitým aspektem je přístup k aplikacím. Při výběru cloudu je možné k datům přistupovat odkudkoliv, kde je zajištěna internetová konektivita. U on-premise řešení je dostupnost aplikací v rukou zákazníka.

Cílem porovnání bylo tyto dvě varianty pouze porovnat – každý uživatel (firma) si musí určit, který model přístupu k aplikacím si vybere. Nelze 100% tvrdit, že jedno je lepší než druhé, a proto výběr vhodného řešení je vždy plně individuální dle potřeb firmy. [54]



Obrázek 15 Porovnání On Premise vs. Cloud, zdroj: [54]

Pro potřeby zavedení nové pobočky v Hradci Králové bylo rozhodnuto, že bude vhodnější zvolit Cloudový přístup díky jeho rychlému nasazení, komplexní správě, nulové pořizovací ceně a plánovanému budoucímu rozvoji firmy.

9.2.4 Výběr vhodných prostorů

Po provedené analýze bylo potřeba před samotnou realizací vybrat a pronajmout vhodný obchodní prostor v centru Hradce Králové. Po krátkém hledání se podařilo zajistit obchodní prostory s celkovou výměrou cca 400 m². Vzhledem k tomu, že v objektu původně sídlila bankovní společnost, tak byl prostor technologicky dostatečně připraven pro potřebné účely. Cílem bylo vybudovat novou pobočku pro již zaběhlou finanční společnost, kde v přízemí bude prostor, který bude poskytovat technické zázemí a směrem do ulice prosklená část tzv. Open Space, která bude určená pro reklamu a zpřístupněná klientům v rámci odborného poradenství. V přízemí se musela vybudovat požadovaná konferenční (zasedací)

místnost, kuchyňka a byla zde připravená zmiňovaná technická místnost, ve které již byl umístěn rack po předchozím nájemníkovi. Dále se v přízemí nacházela místnost pro diskrétní jednání s klienty.

Dále na tuto pobočku navazovalo první patro, kde hned za dveřmi byla menší místnost cca 3×3 m. Tuto místnost lze nazývat jako technickou, jelikož zde byl umístěný další rack a druhá část IT zázemí. V místnosti již byla nainstalovaná klimatizační jednotka a na danou místnost volně navazovala otevřená místnost cca 6×3 m, která měla plnit funkci kanceláře pro administrátora IT. Dále se v jednotce kromě kuchyňky, podél dlouhé chodby, nacházely další místnosti, které měly sloužit jako kanceláře pro manažery a administrativní oddělení. Konkrétně marketingové a účetní oddělení, operativa, kancelář jednatele firmy a jedna místnost navíc sloužící jako záložní sdílená kancelář pro pracovníky, kteří cestují mezi pobočkami (Praha, Brno, Hradec Králové) a mohou potřebovat zařízený prostor k práci. Jedna místnost cca 7×3 m byla vyhrazena jako konferenční. Měla sloužit pro školení, porady, případně v rámci prezentování pro nové obchodní partnery. Celkem tedy 5 kanceláří + druhá zasedací místnost.

V celé budově byl již od pronajímatele integrován kamerový systém a přístupový systém na identifikační karty RFID (Radio Frequency Identification) Každý zaměstnanec dostal k dispozici jednu přístupovou kartu.

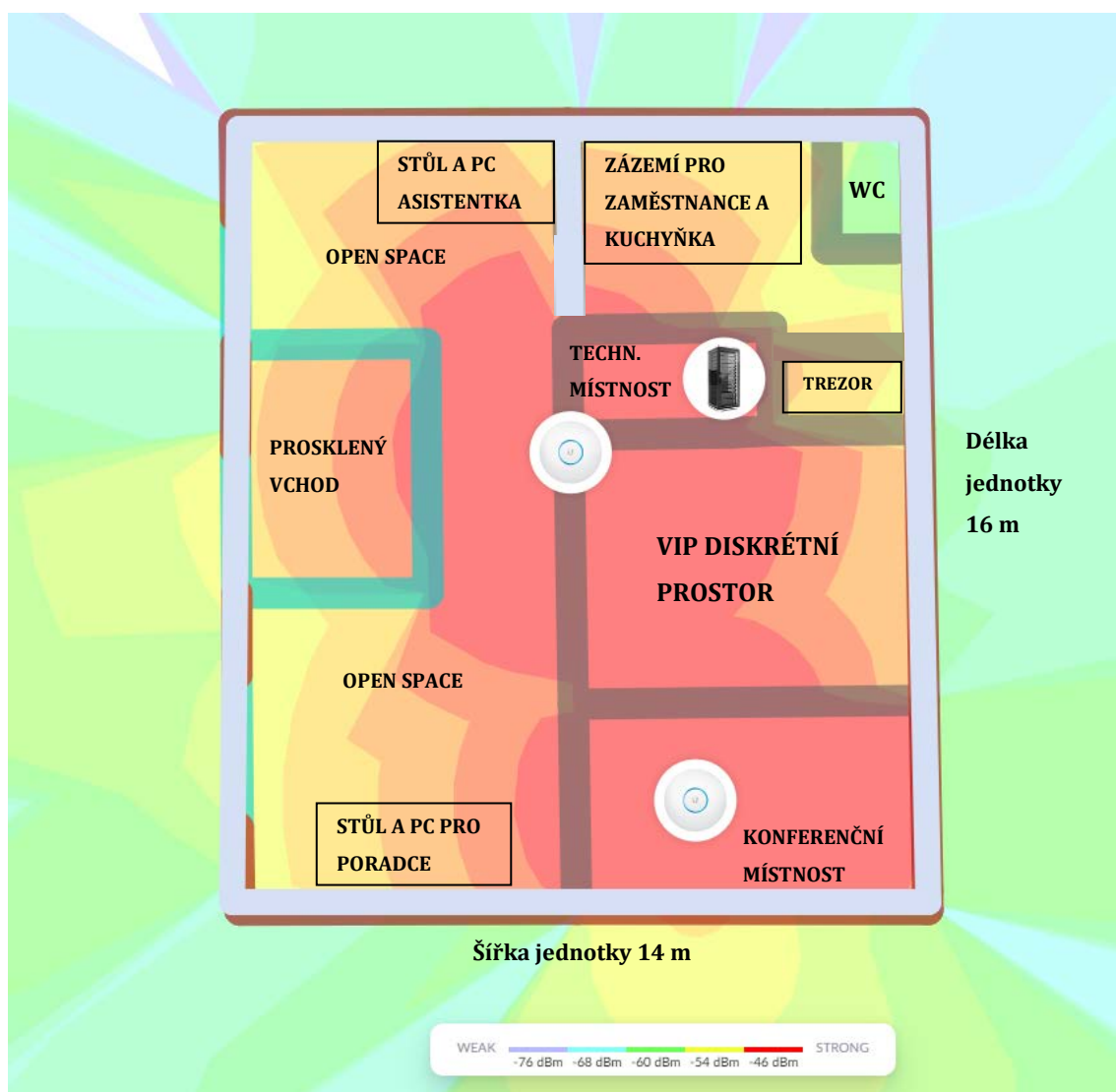
9.2.5 Návrh topologie a umístění síťových prvků na pobočce

Po rozhodnutí, která technologie síťových prvků bude použita pro tuto pobočku, se začalo modelací dle půdorysu této pobočky. Oficiální plány (půdorysy) nebyly k dispozici, proto se tato nájemní jednotka proměřila metrem, promyslely dispozice celé jednotky a dle toho vymýšlelo IT řešení. K vizualizaci a vytvoření tzv. heat mapy se použil online nástroj UniFi® Design Center. Tato heat mapa dle rozměrů jednotky, síly a typu materiálu (sklo, obvodová zeď, příčka) a dle zvolených síťových prvků graficky znázorňuje pokrytí signálem WiFi (Wireless Fidelity) v jednotkách dB.

Níže (viz Obrázek 16) je vidět heat mapa pokrytí přízemí, kde byly umístěny 2 přístupové body. Je zde zakreslená i technická místnost a umístění rack.

VIZUALIZACE PŘÍZEMÍ

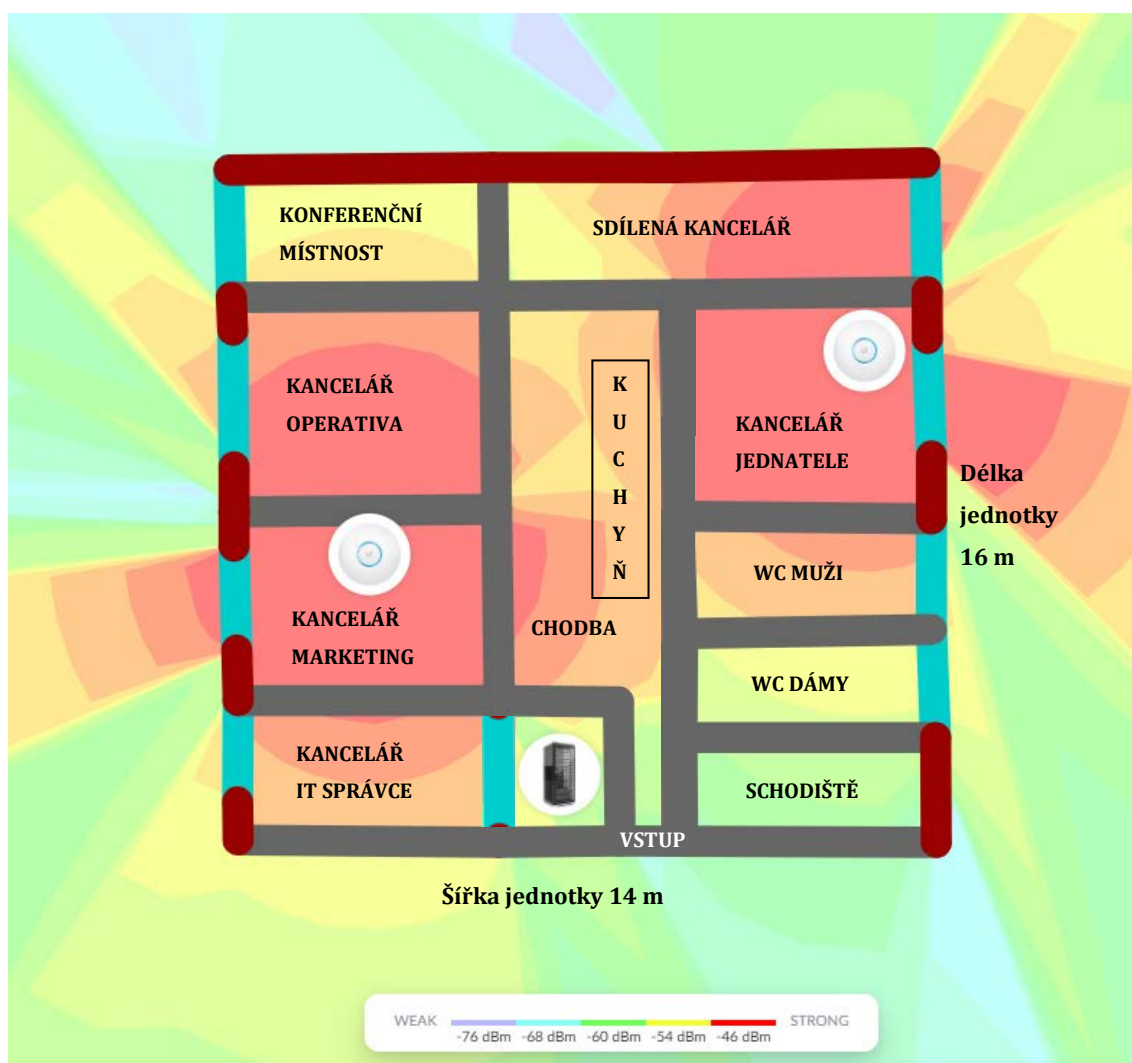
Vizualizace v kombinaci s využitím heat mapy (viz Obrázek 16) znázorňuje detailní pokrytí. Přízemí i první patro má dle měření délku 16 m a šířku 14 m. Pomocí tohoto nástroje se podařilo navrhnout ideální variantu pro požadavky této pobočky. Všechny AP jsou umístěny na stropě a propojeny se switchem. Zároveň bezdrátově komunikují mezi sebou a navzájem skenují kanály ve svém okolí. Do sítě, konkrétně do switchu, je připojen UniFi Cloud Key Controller pomocí kterého se celá síť konfiguruje. Switch, patchpanel (propojovací pole) a router byly umístěny do racku, který se nachází v zabezpečené technické místnosti.



Obrázek 16 Heat mapa přízemí, zdroj vlastní zpracování

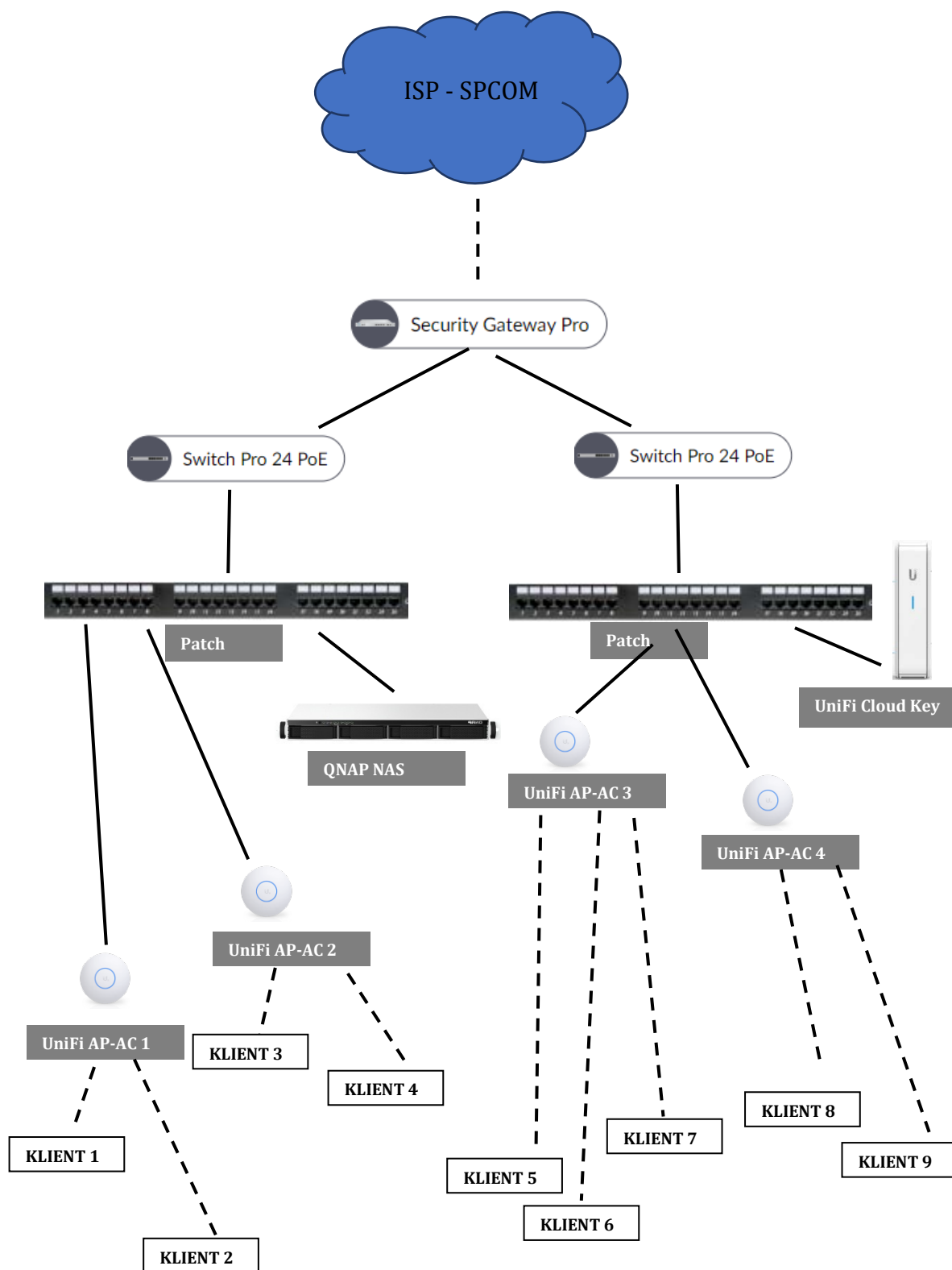
VIZUALIZACE PRVNÍ PATRO

Vizualizace (viz Obrázek 17) znázorňuje dle umístěných AP, kde je nejlepší pokrytí signálu. Na toto první nadzemní podlaží dostačovalo použít 2 AP a bezpečně tak pokrýt celou jednotku o rozloze cca 200 m². Je zde vidět, že nejlepší pokrytí signálu WiFi je v kanceláři jednatele firmy a poté v kancelářích pro administrativní pracovníky (asistentky). Toto umístění AP v prvním patře bylo navrženo i s ohledem na umístění AP, které jsou v přízemí na stropě. Díky tomu je zde i kompletně pokrytá část WC v horním patře i přízemí a část chodby s kuchýnkou v první patře, která je přímo nad AP umístěným v přízemí.



Obrázek 17 Heat mapa prvního patra, zdroj vlastní zpracování

TOPOLOGIE NAVRHOVANÉ SÍTĚ POBOČKY



Obrázek 18 Topologie sítě pobočky, zdroj vlastní zpracování

Síťové připojení z pobočky na ISP (poskytovatel internetu) bylo realizované po 300Mbit lince pomocí radioreléového spoje a zasmulvněno na SLA (Service-level agreement) 99,7 %. Tím bylo zajištěno velice stabilní síťové spojení. Díky většímu kontraktu, při kterém se podařilo dohodnout na umístění antény na střechu budovy a připojení celého objektu i pro ostatní subjekty sídlící v budově za zvýhodněnou cenu (viz Tabulka 2), byl vybrán poskytovatel internetu (ISP) „SPCOM“. V každé místnosti byly ve zdi ethernetové zásuvky, které byly zakončeny v racku v technické místnosti v patch panelu. Vše bylo dobře popsáno a start byl tak znatelně jednodušší. Technická místnost byla připravena i pro průmyslovou UPS. Tato konkrétní technická místnost byla dobře zabezpečena vícero opatřeními. Jmenovitě: koule na dveřích, dveře odolávající požáru, EPS (elektrická požární signalizace), EZS (elektronická zabezpečovací signalizace). V technické místnosti byl taktéž umístěn hlavní rozvaděč. Po detailní obhlídce technického stavu budovy a jednotlivých místností, včetně zaměření signálu a potřebných vzdáleností pro modelaci umístění síťových prvků (konkrétně AP) se začalo s výběrem technologie. Vzhledem k navrhovanému rozpočtu, který byl vyčleněn pro IT řešení a celkovou infrastrukturu se podařilo nalézt, nakoupit a následně implementovat síťové prvky od společnosti Ubiquiti Networks. Zajímavou informací, která vzešla z vyhodnocení průzkumu v dotazníku, bylo, že i většina respondentů by do své společnosti zvolila síťové řešení právě od společnosti UBNT, které velmi dobře odpovídá požadovanému poměru cena/výkon/kvalita.

Síťový hardware, který měl být nakoupen, prošel předem důkladným prověřením dle požadovaných funkcí, specifikací a v poslední fázi prověřením recenzí na zahraničních fórech. Finálně byl zakoupen konkrétně jeden 1U router UBNT USG PRO 4, který kombinuje bezpečnostní bránu, směrovač dat a zabezpečení sítě.

„UniFi Security Gateway PRO kombinuje pokročilé bezpečnostní funkce s vysokým výkonem routování v kompaktním a cenově dostupném řešení. Tento malý směrovač umožňuje až 1 milion paketů za sekundu. UniFi Security Gateway PRO lze snadno konfigurovat pomocí intuitivního softwaru UniFi Controller v4.8+, pomocí kterého lze konfigurovat i jednotlivé UniFi WiFi jednotky.“ Převzato z [55]

Dále se zakoupily dva gigabitové 1U L3 switche UBNT USW-PRO 24 (PRO verze z důvodu aktivního chlazení, přípravy na možný upgrade a výkonné PoE). V rámci pokrytí pobočky byly zakoupeny 4 kusy přístupových bodů UBNT UniFi AP-AC, které umí frekvenční pásmo 2,4 i 5 GHz. Tyto gigabitové AP umí SDN, a tak je jejich implementace velmi pohodlná a rychlá. Zapojení těchto AP proběhlo pomocí standardu PoE. Posledním zakoupeným prvkem v rámci síťové infrastruktury byl UBNT UniFi Controller, Cloud Key (G1).

Všechny síťové prvky se umístily na své místo dle dříve nasimulované mapy pokrytí. Jednotlivé AP byli umístěny na strop, switche a router do racku. Všechna zařízení byla propojena pomocí ethernetového rozhraní a konfigurace těchto zařízení proběhla výhradně pomocí UBNT UniFi Cloud Key Controlleru, kde jsou jednotlivá zařízení připojená do sítě, automaticky detekovaná. Na síťových prvcích jsou aplikované bezpečnostní funkce IPS a DPI. Zabezpečení AP je WPA2/PSK. Rozsáhlé použití VLAN není v této „malé“ síti potřeba, pouze je oddělená síť pro hosty (Guest) tak, aby se tyto sítě vzájemně neviděly.

Rack o velikosti 48U již byl na pobočce implementovaný a osazený patch panely. Po celkové realizaci byl zaplněn z cca jedné čtvrtiny. UPS byla zvolená APC Smart-UPS 1500, konkrétně SMC1500I-2UC. Kapacita UPS je lehce naddimenzovaná, a tak dokáže podržet celou infrastrukturu cca 60 minut. Ve chvíli výpadku distribuční sítě (DS) začne administrátor manuálně vypínat zařízení, která jsou nejméně potřeba. Jako poslední se nechá běžet síť. Z posledních zkušeností při každém krátkodobém výpadku obstála v rámci své kapacity. Výhodou je, že s ní umí komunikovat Qnap NAS, který byl pořízen pro méně důležité zálohy dat. Do tohoto NAS byly vloženy 4 kusy 4 TB disků (2× 4 TB IronWolf, 2× 4 TB WD Red) a byl zde aplikován RAID 5.

9.2.6 Pořízení a výběr hardwaru

Workstation stanice v tomto projektu nebyly využity a pro všechny zaměstnance byly vybrány repasované notebooky od značky Dell, konkrétně modely E7450, E5550 a XPS 13. Prvotně bylo na tuto pobočku zakoupeno 5 ks notebooků pro nové zaměstnance, ostatní zaměstnanci, kteří přešli z jiné pobočky, měli již své vlastní notebooky. Ke každému notebooku se zakoupily originální dokovací stanice od

stejnojmenné společnosti a náhradní napájecí adaptéry. Všechny notebooky jsou vybavené nástrojem BitLocker od společnosti Microsoft a vybrané soubory jsou chráněny pomocí služby AIP (Azure Information Protection), která je součástí balíku Microsoft 365.

Kanceláře byly vybaveny Full HD monitory Dell Professional P2419H s technologií IPS a poměrem stran 16:9. Řada Professional byla zvolena kvůli perfektním ergonomickým stojanům s nastavitelnou výškou a možností otočení na pivot (orientace monitoru na výšku). Monitory jsou opatřeny antireflexní úpravou displeje s možností filtru modrého světla.

Klávesnice a myši byly zvoleny individuálně podle požadavků zaměstnanců, kdy každý z nich měl uvolněný rozpočet na nákup těchto 2 periférií. Nejčastěji však byly vybrány kompletní sady od firmy Dell a Logitech. Ti, co si vybrali vertikální myš, zvolili zařízení Logitech.

Na obou patrech této pobočky byly umístěné velké tiskárny od firmy Kyocera a Xerox. Jako první byla zakoupena použitá černobílá tiskárna značky Kyocera, model ECOSYS M2540dn, bohužel přestal fungovat podavač skeneru, což byl neřešitelný problém, a tak byla zakoupena použitá tiskárna Xerox WorkCentre 5325. V horní části pobočky se využila malá barevná laserová tiskárna od značky Brother, model DCP9020CDW, která byla finančně velmi náročná na provoz. Z tohoto důvodu je nyní používána pouze pro barevný tisk a původní Kyocera byla přesunutá o patro výše.

9.2.7 Výbava kanceláří a konferenčních místností

Do všech kanceláří byly dále pořízené 3segmentové [56] elektrické polohovací stoly se dvěma motory, vyrobené na zakázku od firmy Liftor. Stoly se dají polohovat do výšky od 62 do 127 cm a mají nosnost 100 kg. Na stůl (konstrukci) tohoto typu se dá zvolit jakákoliv deska o velikosti 110 × 60 cm až 180 × 80 cm. Tyto stoly byly zakoupeny se záměrem užívání konkrétními lidmi při výšce, která jim bude vyhovovat, nicméně je zcela reálné, že se postupem času zaměstnanecký tým obmění a u takového stolu lze pracovat i ve stoje, v případě potřeby. Každý stůl byl osazen deskou o velikosti 180 × 60 cm.

Kancelářská křesla byla také pořízena jednotně a pro všechny zaměstnance stejný model MOSH AIRFLOW-702L. Pokud někdo chtěl využít jinou kancelářskou židli, musel si jí pořídit na své vlastní náklady. Vybrané křeslo má nastavení bederní opěrky, hlavovou opěrku a nastavitelné područky. Podmínkou byla možnost nastavení opěradla. Nosnost této židle je až 150 kg.

Konferenční místnosti byla vybavené na zakázku vyrobeným zakulaceným stolem z masivního dřeva o velikosti 4 × 1,2 m. Součástí stolu byl již předem navrhnutý prostup pro kabeláž. Uprostřed stolu 2 integrované lišty s celkem 14 elektrickými zásuvkami. Stůl je navržen pro 14 účastníků konference či porady. Dále bylo do každé zasedací místnosti vybráno 14 textilních křesílek, konkrétně BHM GERMANY Filton na kolečkách. Nejsou sice zdravotní, ale zajišťují pohodlí po celou dobu trvání konference. Pro ozvučení zasedací místnosti byla použita reprosoustava Logitech Speaker System Z906. Jedná se o prostorové reproduktory v sestavě 5+1 o celkovém výkonu 500 W s velmi kvalitním podáním zvuku. Dále byly obě konferenční místnosti vybavené bílou tabulí na kolečkách, projektorem Epson EH-TW650 s full HD rozlišením a poměrem stran 16:9. Plátno pro promítání bylo součástí dodávky projektoru.

9.2.8 Výběr softwarové vybavení

Pro každého zaměstnance byly zakoupeny licence Microsoft 365 a 5 vyvolených zaměstnanců dostalo vyšší verzi, aby mohli využívat Desktopové Office. Notebooky již měli z výroby OEM licenci na Windows 10. Pro těchto 5 zaměstnanců bylo také zakoupeno 5 licencí pro kancelářský balík Adobe Acrobat Pro DC. Všechny licence jsou typu SaaS, které byly pro potřeby firmy ideální.

Nejvíce využívanými softwarovými programy v této firmě jsou: Slack, OneDrive (SharePoint), Outlook, Excel, Word, Adobe. V oblasti účetnictví je využíván licencovaný hostovaný systém Pohoda, který je spravován skrze vzdálenou plochu.

V celé firmě byly zavedeny 2 hlavní komunikační kanály. Microsoft Outlook pro mailovou komunikaci a bezplatná aplikace Slack. „Slack je aplikace pro zasílání zpráv pro firmy, která spojuje lidi s informacemi, které potřebují.“ Spojuje lidi, aby pracovali jako jeden sjednocený tým. Převzato a přeloženo z [57]

9.3 Cenová kalkulace

Cenová kalkulace (viz Tabulka 1) vychází z cen, které byly v době nákupu aktuální (rok 2017). Všechny položky byly nakupované na firmu, přesto jsou zde uvedené s cenami včetně 21 % DPH. V cenové kalkulaci je zmíněn konkrétní produkt, počet zakoupených kusů takového produktu, cena za jeden kus a celková cena za dané položky v jednom řádku. Na konci tabulky se nachází konečný součet za způsobilé náklady. Nejvyšším jednorázovým nákladem byla textilní křesílka a polohovací stoly Liftor. Následující tabulka č. 2 zobrazuje všechny služby, které jsou placené na měsíční bázi. Nejdražší položkou je měsíční poplatek poskytovateli internetu ve výši 9.000 Kč.

Produkt/služba	Počet ks	Cena za ks vč. DPH	Cena celkem vč. DPH
UBNT USG PRO 4	1	7752	7.752 Kč
UBNT USW-PRO 24 - PRO	2	18624	37.248 Kč
UBNT UniFi AP-AC	4	2168	8.672 Kč
UBNT UniFi Controller, Cloud Key (G1)	1	2109	2.109 Kč
APC SMC1500I-2UC	1	21889	21.889 Kč
Qnap TS-431XeU	1	17420	17.420 Kč
WD Red 4TB	2	2499	4.998 Kč
Seagate IronWolf 4TB CMR	2	2472	4.944 Kč
NTB Dell Latitude E7450	2	7990	15.980 Kč
NTB Dell Latitude E5550	2	13660	27.320 Kč
NTB Dell XPS 13	1	41990	41.990 Kč
Dell PR03X Dockstation USB 3.0	4	299	1.196 Kč
Náhradní adaptér k NTB	4	660	2.640 Kč
Dell Professional P2419H	11	5647	32.117 Kč
Set Dell Premier KM7321W	4	2025	8.100 Kč

Logitech G PRO MGK	1	2434	2.434 Kč
Myš Logitech MX Vertical	2	2129	4.258 Kč
Apple Magic Keyboard	1	3244	3.244 Kč
Kyocera ECOSYS M2540dn	1	10890	10.890 Kč
Xerox WorkCentre 5325	1	24000	24.000 Kč
Brother DCP9020CDW	1	8912	8.912 Kč
Polohovací stůl Liftor	11	9999	109.989 Kč
Deska na stůl Hornbach	11	1276	14.036 Kč
Kancelářská židle MOSH AIRFLOW-702L	10	9053	90.530 Kč
Zakázkový stůl do konferenční místnosti	1	13000	26.000 Kč
BHM GERMANY Filton, textil, tmavě šedé	28	4199	117.572 Kč
Logitech Speaker System Z906	2	5990	11.980 Kč
Q-CONNECT 120 × 90 cm	2	6832	13.664 Kč
Epson EH-TW650	2	14822	29.644 Kč
Promítací plátno Aveli	2	1	2 Kč
De'Longhi Dinamica ECAM 350.55 B	2	15490	30.980 Kč
Xiaomi Mi 360° Home Security Camera 2K Pro	1	1201	1.201 Kč
Drobné periferie a prodlužky	15	200	3.000 Kč
CELKOVÁ KONEČNÁ CENA			736.711 Kč

Tabulka 1 Cenová kalkulace vstupních nákladů, zdroj vlastní zpracování

Produkt/služba	Počet uživatelů	Jednotková cena vč. DPH/měsíc	Cena celkem vč. DPH/měsíc
Měsíční poplatek ISP	1	9000	9.000 Kč
Microsoft 365 Business Basic	5	150	750 Kč
Microsoft 365 Business Standard	5	310	1.550 Kč
Adobe Acrobat Pro DC	5	463	4.630 Kč
iPodnik základ	4	332,75	1.331 Kč
Aplikační hosting POHODA	4	205,75	823 Kč
CELKOVÁ MĚSÍČNÍ PLATBA			18.084 Kč

Tabulka 2 Cenová kalkulace měsíčních plateb, zdroj vlastní zpracování

10 Shrnutí

Hlavní pilíře, které měly být v rámci implementace naplněny: Jednoduchý systém, levný systém, bezpečný systém, funkční systém a škálovatelný systém, který není náročný na údržbu.

Po pár letech provozu je možné říct, že toto řešení opravdu bylo úspěšné a splňuje veškeré výše stanované parametry. Celý systém lze velmi jednoduše spravovat na dálku z jednoho místa a IT správce má celkový přehled a kontrolu nad infrastrukturou. Za zmínku stojí zabezpečení systému. Tím, že jsou všechna data uložena na cizích serverech a je s nimi pracováno skrze cloud, tak řešení velmi dobře obstálo při neplánovaném zásahu bezpečnostních složek na anonymní oznámení. Bezpečnostní složky prvně šly po discích a serverech, aby získaly potřebná data. Ovšem překvapením pro ně bylo, že žádné servery nenašly, a tak mohly o data zažádat pouze IT specialistu, který se mohl sám rozhodnout na základě pokynů od majitele firmy a právních zástupců, zdali dá přístupy k datům v

cloudu. Všechny notebooky, do kterých se snažily dostat, byly okamžitě zašifrovány díky BitLockeru.

Kompletní zaštitění IT technologiemi, nábytku a dalšího potřebného vybavení stálo majitele této pobočky 736.711 Kč včetně DPH. Cena byla pro tu danou chvíli konečná. Postupem času se pouze rozšířilo o notebooky, licence pro nové pracovníky, a to byla veškerá investice. Do ceny není zahrnuta práce. Tu kompletně zajišťoval IT administrátor, který zároveň plní funkci opraváře a montážníka v rámci svého fixního platu.

Doporučení pro zlepšení:

Pokud by se dnes tento projekt implementoval znovu, udělalo by se pár změn. Například vybraná UPS nebyla tou správnou volbou a dnes by bylo zvoleno jinak. Důvodem je, že tato UPS má jen Smart Connect, takže ji lze ovládat pouze přes cloud a je třeba zaplatit za to, aby bylo možné ji ovládat. Jedná se o SW novinku, dříve toto nebylo vůbec možné. Tato UPS tedy jen posílá emaily, když vypadne distribuční síť a jedná se jen o určité časové předplatné, které bylo součástí pořizovací ceny. Pokud by ji chtěl IT správce spravovat lokálně po síti, bylo by nutné zakoupit management kartu, která bohužel obnáší další investici cca 16 tisíc Kč. [58]

Také s výběrem tiskárny by se znovu udělal větší průzkum, aby již první model tiskárny byl tou správnou volbou dle požadovaných parametrů firmy, viz záruka, kvalita, cena tisku, pořizovací cena.

Osobně tento projekt hodnotím jako velice úspěšný. Byla vybudována moderní pobočka pro zaběhlou finanční společnost s funkční infrastrukturou jak v rámci IT, tak dalších technických řešení celého managementu. Síť je i s odstupem času (5 let) stále stabilní a zakoupená zařízení až na tiskárnu, která byla zakoupená jako použitá, nadále fungují a plní své úlohy. V projektu byly využity kvalitní produkty, které nebyly nejlevnější volbou na trhu. Za to poskytují patřičný užitek, který přináší menší starosti firmě a umožňují jí tak věnovat se plně jejímu oboru podnikání.

11 Závěr

Na základě stanoveného cíle se podařilo vytvořit komplexní návrh IT ve středně velké firmě, od kterého se může začínající podnikatel či IT správce odrazit a dále si jednotlivé dílčí části nastudovat z další odborné literatury. V práci se podařila zachovat stručnost informací pro přiblížení dané problematiky. Jsou zde zmíněny všechny klíčové body v rámci podkapitol bez rozsáhlého a podrobného vysvětlování.

Pro vytvoření bakalářské práce byly použité odborné texty, dále převzaté či parafrázované informace z internetových publikací a aktuální informace z oficiálních webových stránek výrobců. V bakalářské práci se podařilo zmínit více řešení, které lze uvážit před realizací svého vlastního.

V praktické části bakalářské práce je znázorněn náhled na provozu schopnou, komplexní a reálnou optimalizaci IT pro pobočku středně velké firmy s určitými prvky z oblasti managementu, aby nebylo opomenuto, že mít prosperující pobočku není jen o IT, nýbrž i o dalších aspektech, nad kterými je třeba se zamyslet. Součástí návrhu implementace v praktické části se podařilo vytvořit kalkulaci použitého materiálu při realizaci nové pobočky. S investicí do zmiňované pobočky jsme se dostali pod 1 milion Kč ve vstupních nákladech.

Posledním cílem v rámci realizace byl požadavek na zajištění vzdálené správy z jednoho místa a příprava na možné rozšíření. Tím, že jsou veškeré aplikace provozovány v cloudu a síťové řešení spravované pomocí cloudového controlleru, byl i tento cíl naplněn a správa celé organizace probíhá z jednoho bodu za pomoci vzdáleného přístupu. Implementované řešení nabízí možnost rozšíření infrastruktury o další prvky díky již připraveným kabelovým trasám a volnému místu v racku.

Při realizaci bylo překvapením, jak je časově náročná příprava celého řešení, složitá komunikace IT správce s vedením firmy, a nakonec vydání finálního rozhodnutí o tom, která řešení budou implementována. Při dokončování práce bylo také zjištěno, že nelze vytvořit univerzální koncept a použít jej pro každou středně velkou společnost. Ke každé firmě je nutné přistupovat individuálně.

12 Seznam použité literatury

- [1] STAFF, Hooman. Cloud Computing: The difference between IAAS, PAAS and SAAS. Techrevv.com [online]. 2021 [cit. 2022-01-25]. Dostupné z: <https://techrevv.com/cloud-computing-difference-between-iaas-paas-saas/>
- [2] MANAGEMENTMANIA. ITIL (Information Technology Infrastructure Library). Managementmania.com [online]. 2018 [cit. 2022-07-25]. Dostupné z: <https://managementmania.com/cs/information-technology-infrastructure-library>
- [3] PECINOVÁ, Pavlína. Rozdíl mezi ITIL v3 a ITIL 4. [online]. Zlín, 2021 [cit. 2022-08-01]. Dostupné z: <https://theses.cz/id/01dn2h/>. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce Ing. Lukáš Králík.
- [4] WAWRECZKA, Marek. Přestavba komunikační síťové infrastruktury. [online]. Brno, 2019 [cit. 2022-08-01]. Dostupné z: <https://theses.cz/id/x81j63/>. Bakalářská práce. Vysoké učení technické v Brně.
- [5] KLUBAL, Stanislav. Cloudové hrozby. Hackinglab.cz [online]. 2021 [cit. 2022-07-10]. Dostupné z: <https://hackinglab.cz/cs/blog/cloudove-hrozby/>
- [6] EMPEY, Charlotte. Co je VPN a jak funguje? Váš základní průvodce. Blog.avast.com [online]. 2019 [cit. 2022-08-01]. Dostupné z: <https://blog.avast.com/cs/co-je-vpn-a-jak-funguje>
- [7] MICROSOFT ACADEMY. Microsoft Azure pro začátečníky. Microsoftacademy.cz [online]. [cit. 2022-07-10]. Dostupné z: <https://microsoftacademy.cz/microsoft-azure-zacatecnik-new>
- [8] ŠRAGA, Miroslav. Co je Microsoft 365, čím se liší od Office 365? Blog.dataclue.cz [online]. 2020 [cit. 2022-07-10]. Dostupné z: <https://blog.dataclue.cz/co-je-microsoft-365-cim-se-lisi-od-office-365/>
- [9] GENG LIN, D. FU, JINZY ZHU a G. DASMALCHI. Cloud Computing: IT as a Service. IT Professional [online]. 2009, 11(2), 10-13 [cit. 2022-07-10]. ISSN 15209202. Dostupné z: doi:10.1109/MITP.2009.22

- [10]MICROSOFT. Azure Active Directory. Azure.microsoft.com [online].
[cit. 2022-07-10]. Dostupné z: <https://azure.microsoft.com/cs-cz/services/active-directory/#overview>
- [11]C SYSTEM CZ. Exchange Online. Cloud.csystem.cz [online].[cit. 2022-07-10].
Dostupné z: <https://cloud.csystem.cz/cloudove-produkty/exchange-online>
- [12]Microsoft 365, 2020, What is Microsoft SharePoint and How Can I Use It?,
YouTube video. [cit. 2022-07-10]. Dostupné z:
<https://www.youtube.com/watch?v=QSoEaNG3VJ8>
- [13]CISCO NETWORKING ACADEMY. CCNA: Introduction to Networks. Cisco
[online vzdělávací kurz]. [cit. 2022-07-10]. Dostupné z:
<https://www.netacad.com/courses/networking/ccna-introduction-networks>
- [14]KLEMENT, Milan. VIRTUALIZACE INFRASTRUKTURY POČÍTAČOVÉ SÍTĚ
[online]. Olomouc: Univerzita Palackého, 2007 [cit. 2022-04-19]. Dostupné z:
https://www.researchgate.net/publication/292983530_VIRTUALIZACE_INFRASTRUKTURY_POCITACOVE_SITE
- [15]Eric Spellmann, 2013, How to Choose an Internet Service Provider,
YouTube video. [cit. 2022-08-13]. Dostupné z:
https://www.youtube.com/watch?v=b_9TqLR8fto
- [16]MANAGEMENTMANIA. Router (Směrovač).ManagementMania.com [online].
[cit. 2022-07-10]. Dostupné z:<https://managementmania.com/cs/smerovac-router>
- [17]Tomáš Prekop, 2020, 13 - Model TCP/IP a ISO/OSI referenční model
počítačové sítě, Internet - OBECNÉ POJMY, Youtube video. [cit. 2022-07-10].
Dostupné z: <https://www.youtube.com/watch?v=dL6EkdbJ4NU>
- [18]BMC. OSI Model: The 7 Layers of Network Architecture. BMC.com [online].
[cit. 2022-07-16]. Dostupné z: <https://www.bmc.com/blogs/osi-model-7-layers/>
- [19]PECHO, Peter. Klasifikace dnešních firewallů. Lupa.cz [online]. 2010 [cit. 2022-07-16]. Dostupné z: <https://www.lupa.cz/clanky/klasifikace-dnesnich-firewallu/>

- [20]BOUŠKA, Petr. Cisco IOS 8 - ACL - Access Control List. SAMURAJ-cz.com [online]. 2009 [cit. 2022-07-10]. Dostupné z: <https://www.samuraj-cz.com/clanek/cisco-ios-8-access-control-list/>
- [21] FORTINET. Wireless Intrusion Detection System. Docs.fortinet.com [online]. [cit. 2022-08-13]. Dostupné z: <https://docs.fortinet.com/document/fortiap/7.0.4/fortiwifi-and-fortiap-configuration-guide/961129/wireless-intrusion-detection-system?fbclid=IwAR3zLFzLx5Oen-D5dssaWL4Yr78-aB1eQFwrw6c-fFK0RtwkuHhbildmCi8>
- [22]ELEKTRONICKE-SYSTEMY. Technické parametry kamerových systémů. Elektronicke-systemy.cz [online]. [cit. 2022-07-10]. Dostupné z: <http://www.elektronicke-systemy.cz/technicke-parametry-kamerovych-systemu>
- [23]LI, Chung-Sheng a Wanjiun LIAO. Software defined networks [Guest Editorial]. IEEE Communications Magazine [online]. 2013, 51(2), 113-113 [cit. 2022-07-10]. ISSN 0163-6804. Dostupné z: doi:10.1109/MCOM.2013.6461194
- [24]URBANÍK, Patrik. *Organizace předmětu Internet věcí*. Hradec Králové, 2021. [cit. 2022-07-10]. Dostupné z: <https://theses.cz/id/fgb8xw/STAG96554.pdf>. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu. Vedoucí práce Ing. Pavel Blažek, Ph.D.
- [25]ALZA. RAID disková pole. Alza.cz [online]. [cit. 2022-07-10]. Dostupné z: <https://www.alza.cz/raid-diskova-pole>
- [26]Black Box, 2009, How to pick an IT rack, Youtube video. [cit. 2022-07-10]. Dostupné z: https://www.youtube.com/watch?v=_rQ7X1uPhsg
- [27]UBIQUITI. Board of Directors. Ir.ui.com [online]. [cit. 2022-07-10]. Dostupné z: <https://ir.ui.com/company/board-of-directors>
- [28]UBIQUITI. Work at Ubiquiti. Careers.ui.com [online]. [cit. 2022-07-10]. Dostupné z: <https://careers.ui.com>
- [29]SMARTONE. Profesionální WiFi síť Aruba Networks. Smart1.cz [online]. [cit. 2022-07-10]. Dostupné z: <https://smart1.cz/wifi/>
- [30]EXCLUSIVE NETWORKS. Fortinet. Exclusive-networks.com [online]. [cit. 2022-07-10]. Dostupné z: <https://www.exclusive-networks.com/cz/vendors/fortinet/>

- [31]AWATI, Rahul a Jessica SCARPATI. Deep packet inspection (DPI). TechTarget SearchNetworking [online]. 2021 [cit. 2022-07-10]. Dostupné z: <https://www.techtarget.com/searchnetworking/definition/deep-packet-inspection-DPI>
- [32]OFFIN, Nick. Které technologie utvářejí budoucnost firemní IT infrastruktury? Vseoprumyslu.cz [online]. 2021 [cit. 2022-07-10]. Dostupné z: <https://www.vseoprumyslu.cz/digitalizace/informacni-systemy/ktere-technologie-utvareji-budoucnost-firemni-it-infrastruktury.html>
- [33]HOLČÍK, Tomáš a Jiří KURUC. Jak vybrat monitor: nenechte se zlákat nepodstatnými parametry. Zive.cz [online]. 2017 [cit. 2022-04-19]. Dostupné z: <https://www.zive.cz/clanky/jak-vybrat-monitor-k-pocitaci/sc-3-a-188211/default.aspx>
- [34]ALZA. HP N9K05AE č. 304 Tri-color. Alza.cz [online]. [cit. 2022-07-10]. Dostupné z: <https://www.alza.cz/hp-n9k05ae-c-304-tri-color-d5238208.htm>
- [35]ALZA. Epson EcoTank L15150. Alza.cz [online]. [cit. 2022-07-10]. Dostupné z: <https://www.alza.cz/epson-l15150-d5790102.htm>
- [36]ALZA. Epson 112 EcoTank Pigment Cyan ink bottle azurová. Alza.cz [online]. [cit. 2022-07-10]. Dostupné z: <https://www.alza.cz/epson-112-ecotank-pigment-cyan-ink-bottle-azurova-d5792267.htm>
- [37]U., Jana. Jak vybrat kvalitní kancelářský nábytek. Covybrat.cz [online]. [cit. 2022-07-10]. Dostupné z: <https://www.covybrat.cz/jak-vybrat-kancelarsky-nabytek/>
- [38]MICROSOFT. Získejte nový pohled na produktivitu s Microsoftem 365 a Microsoft Teams. Microsoft.com [online]. 2022 [cit. 2022-07-10]. Dostupné z: <https://www.microsoft.com/cs-cz/microsoft-365/business/compare-all-microsoft-365-business-products>
- [39]STAFF, Ars. Want to use Office on your new iPad Pro? Then you'll need an Office 365 subscription. Arstechnica.com [online]. In: . [cit. 2022-07-10]. Dostupné z: <https://arstechnica.com/gadgets/2015/09/want-to-use-office-on-your-new-ipad-pro-then-youll-need-an-office-365-subscription/>

- [40]MSOFFICE365. Přejděte s firmou na Microsoft Office 365. Ms-office-365.cz [online]. [cit. 2022-04-19]. Dostupné z: <https://ms-office-365.cz/co-si-predstavit-pod-pojmem-office-365/>
- [41]ADOBE. Plány a ceny aplikace Adobe Acrobat DC. Adobe.com [online]. [cit. 2022-04-19]. Dostupné z: <https://www.adobe.com/cz/acrobat/pricing/business.html>
- [42]ADOBE. Plány a ceny pro aplikace Creative Cloud a další informace. Adobe.com [online]. [cit. 2022-04-19] Dostupné z: <https://www.adobe.com/cz/creativecloud/plans.html>
- [43]VEEAM. Proč Veeam. Veeam.cz [online]. [cit. 2022-04-19]. Dostupné z: <https://www.veeam.com/cz/why-veeam.html>
- [44]VEEAM. Řešení zálohování pro malé podniky. Veeam.cz [online]. [cit. 2022-04-19]. Dostupné z: <https://www.veeam.com/cz/smb-backup-solutions.html?ad=menu-products>
- [45]LEVNAPC. Krabicová vs. OEM verze operačního systému Windows. Levnapc.cz [online]. [cit. 2022-04-19]. Dostupné z: <https://www.levnapc.cz/krabicova-vs-oem-verze-os.html>
- [46]MICROSOFT. Porovnání Windows 11 Pro a Home. Microsoft.com [online]. [cit. 2022-04-19]. Dostupné z: <https://www.microsoft.com/cs-cz/windows/compare-windows-11-home-vs-pro-versions?r=1>
- [47]MICROSOFT. Windows Server. Microsoft.com [online]. [cit. 2022-04-19]. Dostupné z: <https://www.microsoft.com/cs-cz/windows-server>
- [48]MANAGEMENTMANIA. SaaS (Software as a Service). Managementmania.com [online]. [cit. 2022-04-19]. Dostupné z: <https://managementmania.com/cs/software-as-a-service>
- [49]LIŠKOVÁ, Lucie. Zavádění ERP systému Helios Green u zákazníka a jeho parametrizace [online]. 2021 [cit. 2022-07-24]. Dostupné z: <https://is.slu.cz/th/v27nt/>. Bakalářská práce. Slezská univerzita v Opavě, Obchodně podnikatelská fakulta v Karviné. Vedoucí práce Kateřina SLANINOVÁ.

- [50] KOŘOUŠKOVÁ, Barbora. INFORMAČNÍ SYSTÉMY V KOSTCE: ERP, CRM, IMPLEMENTACE. Rascasone.com [online]. 2021 [cit. 2022-07-24]. Dostupné z: <https://www.rascasone.com/cs/blog/informacni-systemy-erp-crm-implementace>
- [51] JUŠTA, Jan. Dotazník znalosti moderních produktů pro podnikání. Forms.office.com [online]. [cit. 2022-07-10]. Dostupné z: https://forms.office.com/Pages/ResponsePage.aspx?id=LlSlofTPcUu867RwQl_ZDQTjXgpXxchPiyHmAefiuvNUNjMyRlBRU0VIQ1Y0UktNRERQWDZIMTkyWS4u&fbclid=IwAR0xotNpeVLDhsTI_58_CZaJL4jQd9Yca9Oo7Mmabfdvy_AvFTbtMUQf9zo
- [52] ROVE. CISCO MERAKI MX VS. UBIQUITI UNIFI. Withrove.com [online]. [cit. 2022-07-10]. Dostupné z: https://withrove.com/cisco-meraki-mx-vs-ubiquiti-unifi/?utm_source=rss&utm_medium=rss&utm_campaign=cisco-meraki-mx-vs-ubiquiti-unifi
- [53] RS-Tech, Wireless Vendor Comparison: Ubiquiti vs Meraki vs Aruba. Blog.router-switch.com [online]. 2020 [cit. 2022-07-10]. Dostupné z: <https://blog.router-switch.com/2020/12/wireless-vendor-comparison-ubiquiti-vs-meraki-vs-aruba/>
- [54] LERNER, Mati. Cloud Vs. On-Premise: The Pros And Cons. Ridge.co [online]. 2022 [cit. 2022-06-16]. Dostupné z: <https://www.ridge.co/blog/cloud-vs-on-premise/>
- [55] HARDSOFT. Ubiquiti USG-PRO-4. Hard-soft.cz [online]. [cit. 2022-04-19]. Dostupné z: <https://www.hard-soft.cz/424%7C481%7C796%7C800%7C.d.455401.ubiquiti-usgpro4--unifi-security-gateway-pro-2x-lan-2x-combo-wan-napajeci-kabel.html>
- [56] LIFTOR. Konfigurátor Lifter Up. Lifter.cz [online]. [cit. 2022-04-22]. Dostupné z: https://www.lifter.cz/konfigurator/kancelarske-stoly/k1_2st_ncerna:k2_18mm_12060_dh1334/nohy/
- [57] SLACK. What is Slack? Slack.com [online]. [cit. 2022-04-24]. Dostupné z: <https://slack.com/help/articles/115004071768-What-is-Slack->

[58]APC. UPS Network Management Card 3 with Environmental Monitoring.
Apc.cz [online]. [cit. 2022-04-29]. Dostupné z:
<https://www.apc.com/us/en/product/AP9641/ups-network-management-card-3-with-environmental-monitoring/>

13 Seznam použitých zkratek

ACL seznam povolených/zakázaných akcí

AD Active Directory

AI umělá inteligence

AIP služba Azure starající se o ochranu informací

AP Access Point

APS Advanced Planning and Scheduling

BGP Border Gateway Protocol

BI Business Intelligence

BPM Business Process

BYOD vlastní zařízení donesené do firmy

CAL klientské licence

CRM Customer relationship management

DDOS Denial of service – hackerský útok, který zahltí a znepřístupní službu

DHCP Dynamic Host Configuration Protocol

DMS Document Management

DNS Domain Name Service

DPI hloubková kontrola paketů

EAM Enterprise Asset Management

ERP Enterprise Resource Planning

FPP krabicová verze softwaru

GDPR legislativa o ochraně osobních údajů

HD vysoké rozlišení

HDMI přenosové rozhraní

HRM Human Resource

HW Hardware

Hyper-V virtualizační nástroj společnosti Microsoft

IaaS Infrastruktura jako služba

IDS detekce útočníků

IOS Internetwork Operating System

IoT Internet věcí

IP Internet Protocol

IPS (display) technologie zobrazení

IPS (router) ochrana proti útočníkům

IPSec IP security

ISO mezinárodní organizace vytvářející standardy

ISP poskytovatel internetového připojení

IT Informační Technologie

ITIL Information Technology Infrastructure Library

LAN Local Area Network

MAC (adresa) Media Access Control

MIS Management Information System

MS Microsoft

NAS síťové úložiště

NAT překlad síťových adres
NTB notebook
NVR síťové úložiště kamerového systému
OEM verze softwaru pro výrobce hardwaru
OS operační systém
OSPF Open Shortest Path First
PaaS Platforma jako služba
PC osobní počítač
RAM operační paměť
RDP Remote Desktop Protocol
RFID bezkontaktní přístupové karty
RIP Routing Information Protocol
RW druh přístupu – čtení a zápis
SaaS Software jako služba
SCM Supply Chain Management
SDN Software Defined Network
SLA smlouva o servisu zařízení/služby
SSD pevný disk bez mechanických částí
SW Software
TCP Transmission Control Protocol
UBNT Ubiquiti
UPS záložní zdroj napájení
URL Uniform Resource Locator
VLAN virtuální lokální síť
VOIP Voice over Internet Protocol
VPN virtuální privátní síť
WAN Wide Area Network
WDR záznam s širokým spektrem

WIFI komunikační standard pro bezdrátový přenos dat

Podklad pro zadání BAKALÁŘSKÉ práce studenta

Jméno a příjmení: **Jan Jušta**
Osobní číslo: **I1800791**
Adresa: **Štefánikova 310 8, Hradec Králové – Moravské Předměstí, 50011 Hradec Králové 11, Česká republika**
Téma práce: **Koncept Moderní IT infrastruktury firmy střední velikosti**
Téma práce anglicky: **Concept of a modern IT infrastructure for a medium-sized company**
Vedoucí práce: **Ing. Pavel Blažek, Ph.D.**
Katedra informačních technologií

Zásady pro vypracování:

Úvod
Firemní datová síť (požadavky, normy ITIL, ISO?)
Infrastruktura (datová infrastruktura, propojení poboček, napojení na ISP)
Služby (web, pošta, ERP, ..)
HW požadavky (typy a konfigurace prvků, IoT, cloud?)
SW požadavky (aplikace, licenční plány)
Bezpečnost (fyzická, datová)
Návrh infrastruktury
Závěr

Seznam doporučené literatury:

- 1, Martin Bucksteeg, ITIL 2011, Brno : Computer Press, 2012, ISBN 978-80-251-3732-1
- 2, Vymětal, Dominik, Projekty informačních systémů v podnicích a jejich realizace, Slezská univerzita v Opavě, Obchodně podnikatelská fakulta, 2008, ISBN: 9788072484775
- 3, Allen, Robbie. a Lowe-Norris, Alistair G., Active directory, Grada, Praha, 2005, ISBN: 9788024709734
- 4, Smith Ben, Zabezpečení systému a sítě Microsoft Windows, Brno, Computer Press, 2006, ISBN 80-251-1260-8
- 5, Wendell Odom, Rus Healy, Denise Donohue, CCIE routing and switching certification guide, Indianapolis, Cisco Press, 2010, ISBN 978-1-58705-980-3

Podpis studenta:



Datum: 24.4.2022

Podpis vedoucího práce:



Datum: 24.4.2022