ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Ulrichová** Jméno: **Pavlína** Osobní číslo: **383297**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra ekonomiky, manažerství a humanitních věd**

Studijní program: **Elektrotechnika, energetika a management**

Studijní obor: **Ekonomika a řízení elektrotechniky**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Marketingová komunikace v oblasti moderních trendů správy sítí

Název diplomové práce anglicky:

Marketing communication in the field of contemporary trends in network management

Pokyny pro vypracování:

- síťové prvky a modely jejich správy (kontrolér versus cloud)
- možnosti a omezení moderního přístupu cloudové správy
- určení cílové skupiny uživatelů pro konkrétní typ modelu správy sítí
- ekonomické porovnání jednotlivých modelů správy sítí z pohledu koncového uživatele
- bezpečnostní rizika jednotlivých modelů správy sítí

Seznam doporučené literatury:

G.Tomek, V. Vávrová - Marketing od myšlenky k realizaci
Imad M. Abbadi - Cloud Management and Security

Jméno a pracoviště vedoucí(ho) diplomové práce:

Ing. Radek Hofman, Atlas, s.r.o.

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **26.09.2018** Termín odevzdání diplomové práce: **08.01.2019**

Platnost zadání diplomové práce: **19.02.2020**

Ing. Radek Hofman podpis vedoucí(ho) práce	podpis vedoucí(ho) ústavu/katedry	prof. Ing. Pavel Ripka, CSc. podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Diplomantka bere na vědomí, že je povinna vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

Datum převzetí zadání	Podpis studentky

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra ekonomiky, manažerství a humanitních věd

Marketingová komunikace v oblasti moderních trendů správy sítí

Marketing communication in the field of contemporary trends in network management

Diplomová práce

Bc. Pavlína Ulrichová

Vedoucí práce: Ing. Radek Hofman

Studijní program: Elektrotechnika, energetika a management

Studijní obor: Ekonomika a řízení elektrotechniky

Praha 2019

Poděkování

Ráda bych tímto poděkovala vedoucímu této diplomové práce panu Ing. Radku Hofmanovi, své rodině a přátelům za důvěru, pomoc a podporu, kterou mi poskytli během tvorby této práce.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracovala samostatně a že jsem uvedla veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

V Praze dne 08. 01. 2019 ……..……..

Abstrakt

Tato diplomová práce se zabývá dvěma alternativními metodami ke správě sítí a s nimi související marketingovou komunikací. Práce ve své teoretické části podrobně popisuje oba modely, jejich silné a slabé stránky a taktéž popisuje marketingovou komunikaci a její základní nástroje. V praktické části srovnává obě metody správy sítě, stanovuje jejich pravděpodobné postavení na trhu v blízké budoucnosti a provádí podrobnou segmentaci trhu správy sítí. Segmentace trhu zahrnuje stanovení kritérií, jejich významu a aplikace. V závěru práce je navržen model marketingové komunikace pro cloudový model správy sítě a provedeno krátké ekonomické zhodnocení obou modelů.

Klíčová slova: Správa sítí, Cloud, marketingová komunikace

Abstract

This diploma thesis is focusing on two alternative methods of network management and marketing communication connected with them. Thesis in it's theoretical part describes both models, their strong and weak points a also describes and defines marketing communication and it's basic tools. In practical part thesis compares the two models, determins probable state of network management's market state in near future and performs thorough segmentation of the market. It contains of determination od criteria, their value and application. In the conclusion of the thesis there is proposal of marketing communication for cloud networ managemment and short economic evaluation of both models.

Key words: Network management, Cloud, Marketing communication

Obsah

1 Úvod

Počítačové sítě jsou už mnoho let nedílnou součástí života moderního člověka, i když si ne vždy plně uvědomuje jejich skutečný význam pro náš život. Sítě mají jeden hlavní účel, a to propojovat zařízení a umožňovat komunikaci mezi nimi. Toho využívají lidé dnes a denně už jen samotným připojením se pomocí svého počítače či telefonu na wifi či ethernetový kabel a vstoupením na internet.

Sítě mohou být malé a omezeného rozsahu (např. domácí síť pro elektronická zařízení v rámci jedné domácnosti, vnitřní firemní síť), ale mohou být i velké a komplexní (např. firemní síť napříč geograficky vzdálenými pobočkami, síť internetového připojení v České republice). Komplexní sítě často vznikají vzájemným propojováním menších sítí mezi sebou. Z toho, co bylo řečeno, je poměrně snadné učinit závěr, že počítačové sítě je třeba spravovat a informovat o různých možnostech správy potenciální zákazníky.

Cílem této práce je prostudovat dva různé modely pro správu sítí a pro jeden z nich navrhnout efektivní marketingovou komunikaci.

V rámci teoretické části budou popsány dva představené modely pro správu sítí, tradiční kontrolerový přístup a cloudový přístup, konkrétně princip jejich fungování, jejich silné a slabé stránky a případná bezpečnostní rizika. Současně popíšu pojem marketingové komunikace, tedy o co se jedná, jaký prodělala historický vývoj, a zároveň uvedu výčet vybraných nástrojů marketingové komunikace společně s jejich popisem a možností využití. Tyto nástroje budou představovat množinu možností, ze které bude možno čerpat při sestavování vhodné marketingové komunikace pro zvolený model správy sítě.

Praktickou část této práce lze taktéž rozdělit na dva tematické celky. V tom prvním provedu porovnání obou modelů správy sítě vůči sobě a pokusím se stanovit pravděpodobný vývoj jejich pozic na trhu v blízké budoucnosti. Zbytek praktické části bude věnován stanovení vhodné marketingové komunikace pro jeden zvolený model správy sítě.

Plánovaným postupem je vybrat a stanovit vhodná a relevantní segmentační kritéria trhu a za jejich pomoci definovat cílové segmenty pro jednotlivé modely správy sítě. Na základě těchto cílových segmentů se následně pokusím vypracovat vhodnou synergickou kombinaci nástrojů marketingové komunikace z teoretické části pro efektivní komunikaci právě s těmito cílovými segmenty.

2 Teoretická část

Cílem této části práce je položit s využitím sekundární literatury teoretické základy pro její praktickou část. Nejdříve zde budu definovat, co pojem správa sítí znamená a proč je jí obecně věnována taková pozornost. Dále zde popíši dva rozdílné typy správy sítí, které se v dnešní době nejčastěji využívají. Jejich výhody a nevýhody poté budu dále analyzovat a porovnávat mezi sebou.

Vzhledem k tomu, že po sítích probíhá stále více komunikace a pohybují se na nich citlivá data, budu věnovat část této kapitoly také bezpečnosti a specifickým rizikům hrozícím v jednotlivých modelech správy sítí. A jelikož zamýšleným cílem této práce je marketingová komunikace a propagace jedno-ho z vybraných modelů, se na konci teoretické části zaměřím na definici marketingové komunikace, její využití a také na její vybrané nástroje, které jsou v dnešní době hojně využívané a efektivní.

2.1 Správa sítí – definice, význam

V této práci se budu zabývat dvěma různými přístupy ke správě sítí, budu je popisovat, hodnotit a posléze se získanými údaji dále pracovat v oblasti marketingové komunikace. Než ale k těmto bodům práce přistoupím, je třeba definovat, co se správou sítě myslí.

Jak uvádí článek „Network management – who needs it?“ [1], správa sítí by se dala shrnout jako množina různých aktivit, které zajišťují bezproblémové fungování všech prvků síťových zdrojů. Prakticky to znamená, že správa sítí by měla zajistit nejen to, že síť bude fungovat, ale také to, že bude efektivně využívat své zdroje, dohlížet na jejich dobrý stav a plnit výkonnostní požadavky svých uživatelů.

Svou roli ve správě sítí hrají především tři základní faktory: hardware, software a lidské zdroje, ať už samotní správci sítí, technici nebo v neposlední řadě také sami uživatelé, protože i ti jsou nedílnou součástí sítě. Hardware je ve většině případů to, co je spravováno, software poskytuje nástroje (více či méně automatizované) pro správu a člověk je ten, jenž využívá těchto softwarových nástrojů a celý konstrukt správy sítě zastřešuje. [1]

Jaká je však vlastně motivace pro komplexní a dobrou správu sítě? V počátcích vývoje počítačové techniky nebyla komplexní správě sítí věnována větší pozornost, neboť sítě obsahovaly relativně málo síťových prvků, byly uzavřené a z venku nenapadnutelné a na jejich

výkon nebyl přikládán až takový důraz. Také byly využívány velmi omezenými způsoby, především pro komunikaci a výměnu základních dat. Od té doby se zvýšil nejen počet zařízení, které se do jedné sítě připojují, ale současně se značně rozšířila i škála typů těchto zařízení, jež i přes stejný výsledný účel mohou mít výrazně odlišné charakteristiky (např. způsobené odlišným výrobcem technologie).

V dnešní době by se s trochou nadsázky dalo považovat za síťové zařízení téměř cokoliv. Od klasických počítačů přes chytré televize, telefony až po hodinky nebo třeba termostat v bytě, který se dá ovládat přes aplikaci v telefonu. Pro účel této práce bude podstatnější zajímat se spíše o prvky, které síť tvoří – switche, routery, access pointy, gatewaye – a jejich správu. Dalším důležitým faktorem, který se objevil především díky příchodu bezdrátových sítí a postupně se stal zcela běžným jevem, je skutečnost, že se sítě začaly dynamicky měnit, neboť především přenosná zařízení se často připojují a odpojují a síť se s tím musí nějakým způsobem vypořádat. [1]

Obrázek 1 - Ilustrativní obrázek obecného síťového prostředí [2]

Výsledkem je situace, kdy se udržování takovýchto sítí stává pro člověka bez pomoci softwarových programů nereálné. A právě tyto čím dál komplexnější sítě je nutné nejen spravovat, ale spravovat je přehledně a efektivně. Při dobré správě sítí totiž můžeme odhalit celou řadu možných problémů. Například včas zaznamenat problém či přerušení spojení

a adekvátně na to reagovat nebo i odhalit probíhající útok na síť či citlivá data. Bezpečnost a spolehlivost jsou jen jeden z aspektů, který se v dnešní době velmi cení. [1]

Skutečnost, že management správy sítí je záležitostí aktuální, nicméně postrádající univerzální řešení, dosvědčuje fakt, že jak uvádí společnost Cisco v [12], ISO (International Organization for Standardization) definovalo těchto pět funkčních oblastí, kterým je v této oblasti třeba věnovat pozornost.

Jedná se o následující:

- Chybový management (Fault management)
- Konfigurační management (Configuration management)
- Výkonový management (Performance management)
- Bezpečnostní management (Security management)
- Management využití (Accounting management)

Element, který je nejčastěji v praxi implementován a kterému je mu věnována největší pozornost, je Chybový management. Jedná se o oblast, která se zabývá detekcí chyb, upozorňováním na ně a i do určité míry jejich opravou. Důvod je prostý, pády a nefunkčnosti sítí jsou v dnešní době málo tolerovatelné.

Dalším významným elementem mimo Chybového managementu je pak bezpečnost. Co se v krátkosti týče dalších oblastí definovaných směrnicí ISO, tak Konfigurační management se zabývá nastavením síťových prvků a zařízení. Výkonový management pak sledováním a celkovým vyhodnocováním různých aspektů výkonu tak, že případně upozorňuje na extrémní hodnoty, aby mohl být celkový výkon udržován na přijatelné úrovni. Bezpečnostní management by pak měl zajišťovat, aby přístup do sítí a jejích technologií měli pouze autorizovaní jedinci. A v neposlední řadě Management využití sbírá informace o využití kapacit síťových zdrojů a předává informaci o celkovém využití zdrojů sítě.

Krom teoretického úvodu společnost Cisco v dokumentu [12] uvádí i konkrétní doporučení pro jednotlivé funkční oblasti tak, aby se zvýšila celková efektivita. Osobně považuji za zcela zásadní první dva elementy a měla by jim být věnována nejvyšší pozornost. Tyto první dva body jsou úzce spjaté s Konfiguračním managementem, protože nastavení jednotlivých prvků sítě přímo ovlivňuje její spolehlivost a bezpečnost.

V příštích kapitolách se zaměřím na popis dvou významných přístupů ke správě sítí, které se v dnešní době objevují na trhu.

2.2 Síťové prvky

Jako síťové prvky můžeme označit všechny součásti, které se podílí na hardwarové podobě a provozu sítí. Síťové prvky se dělí na aktivní a pasivní. Pasivními síťovými prvky se míní takové součásti sítě, které sice přenáší data skrze síť, nicméně data neovlivňují ani nijak nemění. Fungují tedy pouze jako fyzické přenašeče. Mezi pasivní síťové prvky patří kabely, konektory, rozvaděče, spojky, atd. [28]

Aktivní síťové prvky jsou potom definovány jako takové prvky sítě, které pracují se signálem v síti, řídí ho, nějakým způsobem ho upravují (např. zesilují) a běžně jsou umístěny v uzlech sítí, které vzájemně propojují. [29] Mezi aktivní síťové prvky jsou řazeny následující:

Router (Směrovač) [31], [30], [32]

Prvek je využíván jako spojnice minimálně dvou sítí (většinou LAN a WAN), které pracují se stejným síťovým protokolem. Router se umisťuje na rozhraní dvou sítí a funguje jakožto komunikační brána pro styk s vnějším světem. Router se může chovat i jako gateway pokud spojuje dvě nezávislé sítě.

Toho dosahuje tak, že směruje packety po sítích. K tomu využívá hlavičky packetů (headers) a vlastní směrovací tabulky (forwarding tables). Routery jsou spolu navzájem v neustálém kontaktu a společně určují nejlepší cestu mezi dvěma zařízeními. Hlavním účelem routeru je řízení provozu v síti. Router je často prvním napadeným místem, pokud dojde k pokusu zaútočit na síť. Routery se často objevují ve spojení s dalším síťovým prvkem, např. běžnou variantou je router se zabudovaným switchem či Wifi router, který spojuje technologie routeru a Access pointu. Je kombinací několika zařízení jako klasického LAN routeru a bezdrátového LAN Access pointu.

Switch (Přepínač) [31], [30]

Switch tvoří společně s routerem dva nejvýznamnější prvky sítí. Úkolem switche je rozšiřovat síť, spojovat její segmenty a filtrovat a směrovat packety mezi těmito segmenty. Funkcionalita je obdobná hubu, nicméně narozdíl od hubu switch rozesílá packety pouze do segmentu, kde se nachází cílová stanice, a ne do všech, díky čemuž neomezuje rychlost sítě tak jako hub. Switch rozesílá packety na úrovni hardwaru a obecně pracuje na druhé a třetí vrstvě ISO/OSI referenčního modelu. Switch neřeší bezpečnost. Jeho zapojením vzniká homogenní síť a bezpečnost je nutno řešit na vyšších úrovních nebo pomocí topologie. Switche se od sebe liší v základu počtem portů (5, 8, 46, 24, 28 nebo 48) a přenosovou rychlostí dat (10, 100 nebo 1000 Mb/s).

Hub (Rozbočovač) [31], [30]

Hub je prvek, jehož účelem je spojovat lokální sítě. Funguje na principu broadcastu, tedy jakýkoliv packet dostane, rozešle ho na všechny ostatní porty bez ohledu na to, kde leží cílové zařízení. Zařízení, které není cílové a obdrží packet, ho zahodí. Díky broadcastovému typu rozesílání packetů hub často způsobuje zahlcení a výrazné zpomalení sítě z důvodu kolizí. Přítomnost hubu v síti snižuje celkovou bezpečnost topologie sítě, neboť potencionální útočník, pokud se dostane na tento síťový prvek, má prakticky přístup k odposlouchávání a sledování veškeré komunikace. V dnešní době se hub již příliš nevyužívá, byl nahrazen switchem.

Bridge (Most) [30]

Úkolem bridge je propojení více lokálních sítí, přičemž bridge by měl zamezovat šíření kolizní domény. Dříve se používal především v kombinaci s hubem, nicméně dnes je toto řešení zbytečné, neboť bylo nahrazeno switchem.

Repeater (Opakovač) [30]

Repeater je síťový prvek, který zajišťuje šíření signálu i na větší vzdálenosti. Každý signál se po určité uražené vzdálenosti utlumuje a zkresluje. Délka této vzdálenosti se pro jednotlivé technologie různí. Vhodně umístěný repeater signál zrekonstruuje a pošle dál tam, kam se za normálních okolností nezvládne neporušen dostat. Repatery lze vzájemně řetězit

a prodlužovat tak dosahovou vzdálenost signálu, nicméně i takovéto řetězení má svůj určitý limit.

Síťový firewall [30]

Síťový firewall je jedním ze základních síťových bezpečnostních prvků. Bývá umístěn na hranici sítě, a pokud je správně nastaven, poskytuje dobrou základní ochranu sítě před útočníkem. Firewall kontroluje všechny příchozí packety, a pokud některý z nich nevyhovuje bezpečnostním politikám, je zahozen.

Access Point [33]

Wifi Access point (AP, WAP) neboli přístupový bod je zařízení, které poskytuje wifi signál a zajišťuje připojení bezdrátových zařízení k síti. Účelem Access pointu je pokrytí určeného prostoru wifi signálem a standardně se užívá v kombinaci s routerem.

A právě primárně přístupy pro správu těchto aktivních síťových prvků se bude tato práce zabývat. V následujících kapitolách budou tyto přístupy podrobněji popsány.

2.3 Model správy kontrolerového typu

Tento model je často označován jako „tradiční“ způsob správy sítí. Dodnes je to stále velmi používaný způsob, i když v posledních letech musí čelit útokům na svou pozici kvůli nastupujícím cloudovým řešením pro správy sítí. To zapříčiňuje pomalý pokles kontrolerového typu správy na trhu stejně tak jako obecně „tradičních řešení“. Více se o situací na trhu a jejím předpokládaném vývoji bude zabývat kapitola 3.2. Předpokládaná budoucí pozice jednotlivých modelů správy sítí.

Většinu informací pro tuto kapitolu jsem načerpala v praxi a v předchozím studiu.

2.3.1 Popis principu modelu a jeho prvků

Kontrolerovým přístupem ke správě sítí bude v této práci míněn způsob přímého připojování se na jednotlivé prvky sítě a následné ruční nastavovaní, upravovaní na požadované konfigurace či pouze kontrola stavu prvku jestli je v pořádku. A to pro každý síťový prvek zvlášť. Síťová zařízení mohou a nemusí mít vlastní programy pro správu či pro přístup, zvláště pokud jsou síťové prvky od různých dodavatelů. Většinou se ale administrátor nevyhne alespoň různým VPN zabezpečeným připojením, protože pokud prvky neleží v jedné sítí, bude potřebovat ověřený přístup do dané konkrétní sítě. Není možné, aby byly síťové prvky jednoduše přístupné pro každého.

Obrázek 2 - Popis součástí síťových infrastruktur a operací na nich prováděných [34]

2.3.2 Možnosti a omezení využívání tohoto modelu

Jednou z největších výhod kontrolerového přístupu ke správě je právě fakt, že přímo pracuje s jednotlivými prvky sítě, a tudíž má administrátor/správce mnohem větší volnost a může nastavit na míru svým potřebám i takové věci, které by mu cloudový přístup správy vzhledem ke své generičnosti nemusel umožnit.

Výhodou i nevýhodou tohoto přístupu může být otázka zabezpečení dat a komunikace. To v tomto případě bude v rukou správců a administrátorů zákazníka. Data sice neprochází skrze nástroj třetí strany, ale zároveň zabezpečení pak bude přesně na takové úrovni, jakou si zákazník sám nastaví. A to se může případ od případu výrazně lišit. Obecně lze však říci, že zákazník má

málokdy zabezpečení těchto elementů na takové úrovni jako velcí poskytovatelé cloudových řešení, jako je Microsoft, Amazon nebo Google. [24]

Jako jasné omezení musíme pak vnímat fakt, že zákazník musí své zařízení a nástroje, které si zvolil pro jeho správu, udržovat sám aktuální, to jest updatovat je, udržovat a zajímat se o případné objevené bezpečnostní chyby a přijímat proti nim patřičná opatření. Stejně tak si zákazník musí dělat zálohy nastavení a konfigurací sám.

Z finančního hlediska přináší kontrolerový typ ušetření povinnosti platit měsíční či roční platby za využívání cloudových nástrojů a z dlouhodobého hlediska pro některé subjekty stále vychází finančně příznivěji. Například kontrolerové řešení je vhodné pro malé sítě, kde počet prvků ke správě není příliš velký a správa není příliš časově náročná i se samostatným logováním na jednotlivé prvky. Naopak čím více prvků je třeba spravovat, tím více se budou časové prodlevy při přihlašování projevovat.

2.4 Model správy cloudového typu

Cloudový přístup je moderní a nastupující alternativou k tradičnímu řešení nejen správy sítí, ale například i k ukládání dat, kterým je v současné době i nejvíce proslulý, nebo třeba k poskytování služeb a softwaru. [13]

2.4.1 Popis principu modelu a jeho prvků

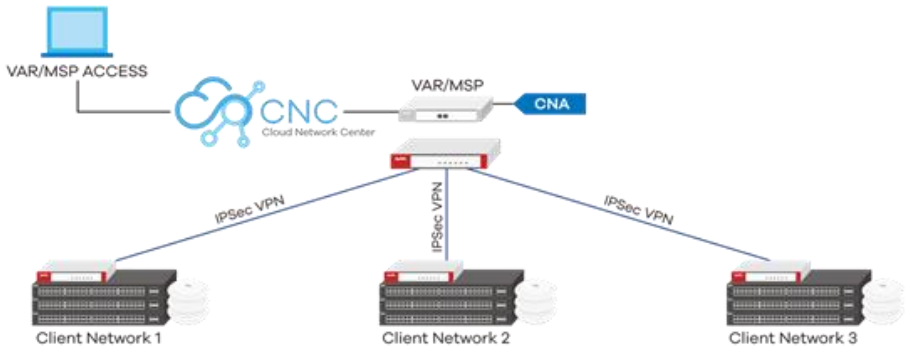
Jak již bylo řešeno v úvodu této práce, spravování sítí se především ve firmách stává stále náročnější činností vzhledem rostoucí komplexnosti, velikosti a množství sítí. Zvláště pak, pokud se jedná o vzdálenou správu, kdy sítě leží v několika lokalitách, ne-li přímo zemích.

Obecně se jedná o řešení, kdy zákazník využívá sdílení zdrojů, služeb či aplikací vzdáleně přes zabezpečené internetové připojení a často platí pouze jen za to, co skutečně využívá. [13] Platby většinou probíhají ve formě měsíčních či ročních nákupech licencí pro žádané služby.

Cloudová řešení bývají obecně rychlá, spolehlivá a v některých případech odstiňují zákazníka od některých nutných povinností, jako je například správa a aktualizace technologií či jejich nákup. Základní myšlenkou cloudu je možnost pronajmout si od cloudového

poskytovatele hardware či software, který firma či obecně zákazník potřebuje, a to jen v takové míře, kterou skutečně využije. Nesmírnou výhodou je potom i velmi dobrá dostupnost prakticky odkudkoliv a kdykoliv.

Cloudový přístup ke správě sítí je v této práci chápán jako po internetu dostupný nástroj, pomocí kterého je uživatel schopen skrze internet spravovat vzdáleně svou síť či sítě. Ideálně vše skrze tento jediný nástroj. Příklad takovéto cloudové správy pro více různých sítí je ilustrován na Obrázku č.3. Toto konkrétní řešení umožňuje vzdáleně jedním centrálním nástrojem spravovat prvky sítě od switchů, access pointů až po gatewaye.



Obrázek 3 - Příklad cloudového řešení správy sítí [16]

2.4.2 Možnosti a omezení využívání tohoto modelu

Mezi nesporné výhody cloudových řešení patří jejich jednoduchost. Poskytují jednoduchý zabezpečený vzdálený přístup k sítím většinou skrze internet – může se jednat o přístup skrze internetový prohlížeč nebo specializovaný software společnosti poskytovatele. Samozřejmě pak vyvstává otázka, jak jsou zabezpečeny všechny prvky, kterými komunikace probíhá. [9]

Cloudová řešení jsou i velmi přátelská co se týče flexibility pracovních postupů. Jsou velice snadno přístupná, prakticky odkudkoliv a z různých zařízení. Jako takové je toto řešení v podstatě nezávislé na platformě a operačním systému. Vzhledem k tomu, že většina těchto aplikací funguje skrze internet a např. webový prohlížeč, který obecně funguje stejně téměř

všude, je samotné využití služby dostupné ve stejný čas v pod-statě kdekoliv. Dalším nesporným kladem je potom existence dobrých a spolehlivých záloh. Cloudový poskytovatelé mívají zpravidla mnohem lépe vyřešené a zabezpečené zálohování dat a konfigurací, než bývá zvykem ve firmách, které se o své zdroje starají sami. [13]

Samozřejmě každý přístup má nejen své výhody, ale i nevýhody. V tomto případě je to primárně otázka internetového připojení, neboť pokud není funkční, není možné se k nástrojům pro správu sítě jakkoliv dostat. Podobný problém nedostupnosti může nastat i v případě, že nastane výpadek na straně poskytovatele cloudového network managementu (či v extrémním případě kdyby přestal náhle existovat). Zákazník se stává závislý na službách třetí strany a problémy poskytovatele se často promítnou např. zmíněnou nedostupností i do záležitostí zákazníka.

Dalším poměrně běžným a diskutovaným nedostatkem pro cloudová řešení je otázka bezpečnosti komunikace a případně dat. V neposlední řadě pak také fakt, že cloudově využívané aplikace lze uživatelsky přizpůsobovat jen do určité míry, která je často mnohem nižší než u klasických aplikací u klienta. [9] Podobně jako výpadek internetu může být problémem u cloudových služeb cílený DoS (Denial of service) útok na poskytovatele služeb, který cílí na to, aby zákazníci měli svou službu nepřístupnou. [13]

Pro lepší porozumění cloudovým řešením jsem shrnula možné modely cloudových řešení. Pro toto shrnutí jsem vycházela ze zdrojů [13], [23] a [26].

Software jako služba (Software as service, SaaS)

Jedná se o poskytování služby, která umožňuje využívání softwaru, který běží na vzdálených serverech, a uživateli je dostupná skrze internetové spojení. Jinými slovy SaaS poskytuje finální produkt/plnohodnotnou aplikaci uživateli, který tuto službu využívá. Tyto aplikace většinou vypadají pro všechny své uživatele téměř stejně a SaaS obecně představuje nejméně přizpůsobitelnou vrstvu. Výhodou, ale i nevýhodou je potom přesunutí odpovědnosti za instalaci, správu, podporu a rozhodování o instalaci updatů do rukou poskytovatele. Je ovšem dobrým zvykem před významnějšími updaty zákazníka o času, rozsahu a případném dopadu informovat.

SaaS je v současnosti největší z cloudových segmentů a generuje více než polovinu tržních příjmů tohoto odvětví. [23] Běžně se jedná o takové aplikace jako firemní software nebo

například webově založený emailový klient. Software se většinou nakupuje skrze předplatné. Typickými poskytovateli SaaS služeb jsou například Salesforce, Google Docs, Microsoft Office 365, Basecamp, Adobe a další. Typickými zákazníky pak jsou firmy, které využívají hodně běžných softwarů.

Platforma jako služba (Platform as service, PaaS)

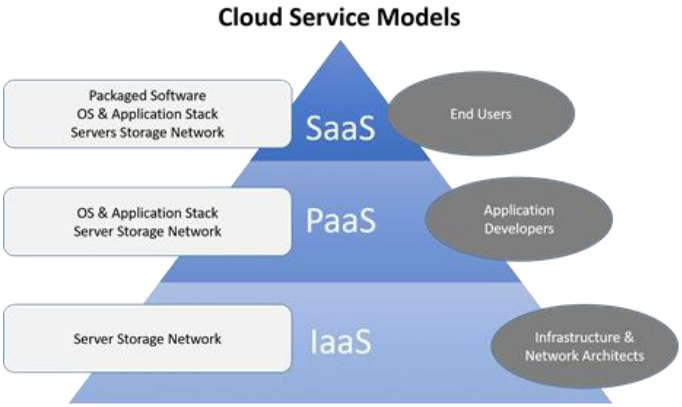
Smyslem tohoto cloudového modelu je online rozvoj schopností vytvářet a upravovat aplikace tak, aby vyhovovali firemním potřebám. Součástí je hardware, databáze a softwarové vývojové nástroje – souhrnně označované jako „cloudware". PaaS nabízí služby, které nejsou určeny přímo pro koncové zákazníky, nýbrž pro vývojáře a vývojem se zabývající oddělení firem. Může se jednat o škálu různých produktů, od serveru pro autentizaci uživatelů, přes službu pro komunikaci mezi jednotlivými části aplikace až po služby na monitorování dostupnosti těchto aplikací.

Největší sílou tohoto modelu je to, že umožňuje rychlejší vývoj nových věcí a poskytuje pestrou škálu různých nástrojů, které může snadno rozšiřovat. Stejně jako u ostatních cloudů jsou zde zdroje uloženy vzdáleně a přistupuje se k nim skrze webové rozhraní. Příkladem poskytovatelů PaaS jsou typicky Salesforce, Amazon Web Service (AWS), Microsoft Azure, IBM BlueMix nebo Google App Engine.

Infrastruktura jako služba (Infrastructure as service, IaaS)

Tento model nabízí využívání virtuálních prostředků, které běží na již existujícím serverovém hardwaru, síťovém hardwaru nebo prostoru pro ukládání dat vlastněném poskytovatelem. Lze tak velice efektivně sdílet velkokapacitní hardwarové zdroje mezi více zákazníků a efektivně tak využívat fyzický hardware jak z hlediska volných zdrojů, tak z hlediska snižování nákladů na celkové pořízení a správu.

IaaS je svou velikostí trhu roven přibližně polovině SaaS trhu, nicméně průzkumy ukazují, že stále více firem vyhledává cloudové IT infrastrukturní řešení namísto těch tradičních. Jednou z velkých výhod proti ostatním modelům služeb je to, že IaaS model je na poměry cloudu velmi dobře customizovatelný. Typickými zástupci poskytovatele služeb IaaS jsou například Amazon EC2, Rackspace, Google Computer Engine a další.



Obrázek 4 - Přehled zákaldních cloudových modelů [18]

Je samozřejmostí, že cloudová řešení neexistují pouze v tomto základním striktním dělení. Potřeby jednotlivých podniků se od sebe liší, a proto se nezřídka objevují i hybridní řešení. Prodejci, kteří nabízí více modelů, jsou například Salesforce (nabízí IaaS a PaaS varianty) nebo Amazon Web Services (nabízí varianty IaaS a PaaS).

Předpokládá se, že v příštích pěti až deseti letech se bude vývoj cloudových řešení výrazně zabývat především tím, jaké kombinace těchto modelů a v jaké míře budou pro trh a jeho zákazníky nejlákavější.

Díky této charakterizaci lze říci, že cloudový přístup ke správě sítí tak, jak byl definován výše, spadá do kategorie SaaS cloudového modelu a sdílí jeho silné a slabé stránky. Příkladem dostupného cloudového řešení pro správu sítí v České republice je například Cloud networking center (CNC) nabízený firmou Zyxel (obrázek č. 3 v kapitole 2.4.1.). [16], [27]

2.5 Bezpečnost správy sítí

2.5.1 Obecná bezpečnostní rizika a možnosti obrany

Počítačová síť aneb prostor, který umožňuje počítačům si vyměňovat data, v dnešní době představuje něco tak základního, že si život bez ní jen stěží umíme představit. Přestože s sebou tato technologie nese obrovskou míru možností a výhod, současně s tím ruku v ruce jdou i jistá

rizika. V tomto případě rizika, především bezpečnostní. Mnohdy totiž sítí putují citlivá osobní data, která v nesprávných rukou mohou způsobit nemalé potíže.

Jak už bylo řečeno, počítačová síť je spojení často velkého počtu uzlů/výpočetních prvků, které jsou vzájemně propojeny ať už kabelovou, či bezdrátovou technologií [8]. Z logiky věci je patrné, že takováto struktura nemůže fungovat bezproblémově sama o sobě. Je třeba tyto zdroje a uzly náležitě spravovat a koordinovat jejich činnost a výkon za účelem nepřetržitého spolehlivého provozu. A přesně to označujeme jako správu sítí (network management). Problém, se kterou se správa sítí potýká skoro nejčastěji, je otázka bezpečnosti, za níž by měla ručit právě správa síťových systémů.

Dle [8] a [9] mezi nejběžnější bezpečnostní problémy sítí patří následující:

- Udržení celkové integrity (bezúhonnosti) sítě.
- Únik dat.
- Zabránění a předcházení pronikání neautorizovaných jedinců do systému a následné odposlouchávání nebo odcizení citlivých dat (osobní údaje, hesla, atd.).
- Útoky, hackování a viry.
- Zajištění ochrany systémů před DoS (Denial of service) a DDoS (Distributed Denial of service) útoky z vnějšku.
- Velikost samotné sítě. Čím větší síť je, tím více zranitelných míst má a tím více narůstá bezpečnostní riziko. Možnými zranitelnými místy může být počet uživatelů, hardware či další.
- Nákladnost investice do odpovídajících obranných prvků – firewally, proxy, fyzická ochrana hardwaru. Často míra zabezpečení souvisí úzce s otázkou rozpočtu.

Je jasné, že není možné vždy perfektně zabezpečit síť proti všem možným potenciálním hrozbám. Příčin je vícero [9], jde jednak o praktické důvody, kdy obecně platí, že nikdy neexistuje něco jako dokonalá obrana, neboť se najde způsob, jak ji prolomit. Dalšími jsou důvody ekonomické, kdy se odborník či spíše manažer může dostat do situace, kdy další náklady na zabezpečení sítě budou neúměrně vyšší než finanční náklady a problémy, které by mohly kvůli této hrozbě vzniknout. Cílem by tak nemělo být vytvoření dokonalé obrany proti všem útokům za každou cenu, ale vytvoření obrany přiměřené reálně hrozícím bezpečnostním rizi-

kům, především s přihlédnutím k charakteru sítě a jejímu využití. Malá domácí síť například nebude potřebovat stejnou ochranu jako síť banky.

Pro vyhodnocení toho, které z bezpečnostních opatření má smysl aplikovat, je dobré nechat provést IT assesment [10], jenž má za úkol zhodnotit všechna rizika hrozící danému konkrétnímu projektu, zhodnotit míru pravděpodobnosti jejich výskytu a dopady, které by uskutečnění se dané hrozby přineslo projektu. Na základě těchto tří faktorů, tj. pravděpodobnosti výskytu, cena a dopadů uskutečnění hrozby, se pak jednotlivým rizikům přiřazují riziková označení. Takovýto risk assesment se označuje za kvantitativní. Kvantitativní risk assesment je možné a vhodné používat právě tehdy, pokud jsou k dispozici dobrá a přesná data.

Bohužel v praxi k tomu tak často nedochází, protože např. většinou chybí spolehlivá historická data o výskytu jednotlivých rizik. V takovém případě je vhodné využít risk management kvalitativní [10], při němž odborníci využívají svého úsudku k určení pravděpodobnosti výskytu určitého rizika na předem definované škále. Na závěr hodnotícího procesu pak už jen zbývá posoudit, která rizika budou v projektu správy sítí akceptovatelná a která bude třeba řešit nějakou formou obrany.

Mezi nejčastěji obecně platné formy obrany proti bezpečnostním rizikům patří dle [9] následující oblasti:

- Bezpečnostní zařízení (firewally nebo antiviry).
- Bezpečnostní nastavení routeru, operačního systému.
- Záloha dat (off-side).
- Šifrování citlivých dat – ideálně veškeré komunikace.
- Omezení přístupu do síťové infrastruktury na oprávněné osoby.
- Trénink oprávněných osob v bezpečném používání technologie, aplikace politika správných pravidel pro užívání.
- Pravidelná údržba sítě.

Mezi jeden z nejrozšířenějších a nejpoužívanějších způsobů obrany před bezpečnostními riziky jsou firewally [11]. Uvedu je zde jako příklad. Firewally mohou být softwarové i hardwarové povahy a jejich účelem je filtrovat příchozí a odchozí provoz dat na síti. Firewall

takto může poměrně efektivně blokovat např. pod-vodné či fishingové emaily, stahování malwaru do zařízení, přístup na zakázané stránky nebo pokusy o připojení se z neautorizovaných zařízení. Pokud pak pro zajímavost porovnám silné a slabé stránky firewallů, liší se i mezi typy. Hardwarový firewall je fyzická součást. Buď se jedná o samostatné zařízení, nebo je implementovanou součástí routerů. Hardwarový firewall poměrně dobře chrání celou lokální síť, a to ve své minimální nutné konfiguraci. Je tedy možno ho využívat i s pouhým minimem konfiguračních zásahů, nicméně pro zvýšení zabezpečení je nutno firewall i tak adekvátně nastavit.

Softwarový firewall je pak nainstalovaný přímo v systémech počítačů nebo zařízení. Povětšinou bývá součástí přímo operačního systému. Zde je nutná větší konfigurace, aby síť dobře fungovala.

Pro potřeby této práce je vhodné se podívat nejen na obecná síťová rizika, ale i na konkrétní běžné útoky. Přehled různých typů síťových útoků prezentuje [35] a současně je dělí na dva základní typy, a to na aktivní útoky a pasivní útoky. Za aktivní útoky se považují takové útoky, kdy útočník iniciuje příkazy za účelem narušení normálního fungování sítě (např. DoS, Wormhole attack, Sybil). Pasivními útoky jsou pak útoky, kdy útočník pouze odposlouchává a sleduje data putující po síti (např. Monitoring, Eavesdropping).

2.5.2 Bezpečnostní rizika pro model kontrolérového typu

Jak vyplývá z informací v kapitole 2.3.2., kromě obecných bezpečnostních rizik je pro model správy kontrolerového typu významným bezpečnostním rizikem lidský faktor. V rámci kontrolerového typu správy se administrátor přihlašuje přímo na jednotlivé prvky a má na nich více možností, jak je nastavovat a upravovat konfigurace, než je možné u cloudových nástrojů, které poněkud trpí na svou větší či menší generalizaci. Na jednu stranu má administrátor větší možnosti pracovat se síťovým prvkem do jeho maximálního potenciálu, na stranu druhou se velmi snadno se může stát, že nepozornost, jedno špatné nastavení či ukliknutí může způsobit bezpečnostní díru, přes kterou se útočník může dostat do celé sítě.

Jak už bylo zmíněno v 2.3.2., v případě kontrolerového typu správy přechází odpovědnost za všechna bezpečnostní opatření včetně pravidelných aktualizací do rukou zákazníka. Zcela reálným rizikem tedy může být situace, kdy zákazník nedokáže svá data a komunikace dostatečně zabezpečit.

2.5.3 Bezpečnostní rizika pro model cloudového typu

Pro cloudový model správy sítě jsou asi nejvýraznější bezpečnostní hrozbou útoky cílící na síťovou komunikaci, tedy pasivní síťové útoky. Cloudová řešení obecně stojí na komunikaci zákazníka s poskytovatelem skrze internetové spojení a útok na síťovou komunikaci představuje významnou hrozbu. Takovými útoky narušujícími bezpečnost cloudového přístupu mohou být například Spoofing a Man in the middle útoky.

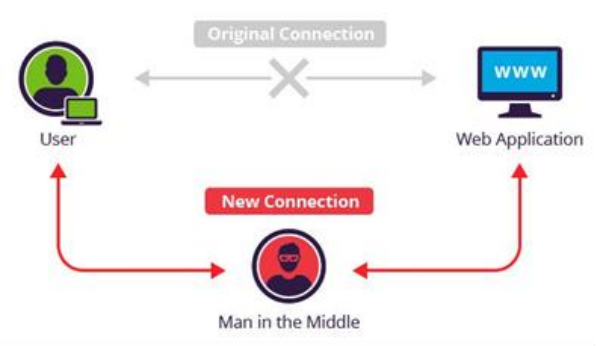
Man in the middle [20]

Jedním z velkých typických rizik pro model cloudového typu je například útok „Man in the Middle“ neboli „Muž uprostřed“ (viz. Obrázek č. 19), jak uvádí [20], ze kterého budu z velké části v této podkapitole čerpat.

Jedná se o typickou hrozbu pro počítače nebo například online služby, mezi které cloudové poskytování služeb bezesporu patří. Jak již bylo totiž řečeno, ve valné většině případů se ke svým zdrojům zákazník připojuje právě skrze internet.

Ve své podstatě se jedná o jednoduchý útok, kdy se útočník nebo útočníkův software dostane mezi uživatele a jeho zdroj informací. Skrze toto narušení informační cesty pak může získávat útočník různé citlivé informace napadeného uživatele či informace o jeho chování. Další možností, kterou útočník může provést s informacemi získanými od uživatele, je manipulace. Útočník zachytí data vyslaná uživatelem, změní je tak, aby to pro něj bylo výhodné, a tyto zkreslené informace následně přeposílá webové službě.

Největší riziko tohoto útoku je nevědomost komunikujících stran. Ani jedna většinou netuší, že komunikace probíhá přes prostředníka, a tento fakt se většinou dost špatně zjišťuje. Základní myšlenka je jednoduchá a zobrazena na Obrázku č. 19, nicméně v praxi existují různé způsoby, jak tento útok realizovat např. ARP Cache poisoning, DNS Spoofing, Roughe DNS útok a další.



Obrázek 5 - "Muž uprostřed" typ útoku na webové aplikace [19]

Spoofing [35]

Dalším typem útoku je spoofing. Jedná se o útok, při kterém útočník vytvoří falešnou verzi například přihlašovacího formuláře do cílového autentizovaného systému a umístí ji na zdánlivě podobnou adresu jako je adresa skutečná. Tuto adresu potom zašle nic netušícím obětem útoku, nejčastěji ze zdánlivě důvěryhodné e-mailové adresy. Pomocí tohoto klamu získává útočník od uživatelů různé informace např. jejich přihlašovací údaje na cílový server, za který se útočník vydává. Útočníci často vizuálně imitují stránky a chování cílových serverů.

Denial of Service [35]

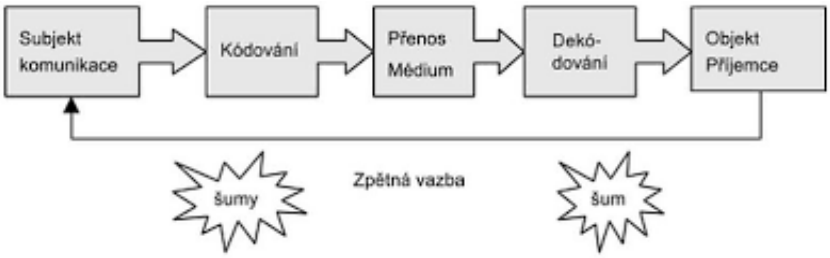
Cloudové řešení není náchylné pouze na pasivní útoky. Velmi nepříznivě ho může ovlivnit také například útok cílený na stranu poskytovatele jako např. Denial of Service útok (DoS). Jak jsem již uvedla v kapitole 2.4.2., hlavním cílem DoS je zahltit cílový server natolik, že pro zákazníka budou jeho služby nepřístupné z důvodu přetížení. V případě cloudové správy sítě by to znamenalo, že pokud útočník zaútočí na servery poskytovatele, zákazník nebude moci spravovat svá zařízení do doby, než útok buď přestane, nebo mu bude zabráněno.

2.6 Marketingová komunikace – definice, využití

2.6.1 Definice a význam

Komunikace je v dnešní době jeden z klíčových faktorů, který neoddělitelně patří k řízení organizací nejrůznějšího zaměření. Často je to právě komunikace s veřejností, která tvoří z velké

části image firmy a ovlivňuje, ať už pozitivně, nebo negativně, postoj zákazníků k organizaci [3]. A právě postoj zákazníků k organizaci hraje v současnosti čím dál větší roli.



Obrázek 6 - Process předávání infromace od původce k příjemci

Velký slovník marketingové komunikace [4] definuje marketingovou komunikaci jakožto čtvrtou ze složek marketingového mixu podle P. Kotlera (viz. Obrázek č. 7), konkrétně „promotion“ neboli propagaci, případně „communication“ alias komunikaci, pokud se díváme analogicky z pohledu zákazníka. Marketingový mix je jedním z nejpoužívanějších metod pro třídění a výběr vhodných marketingových nástrojů [3].

Obrázek 7 - Marketingový mix dle P. Kotlera [5]

Trochu detailnější a podrobnější definici lze nalézt v knize Marketing – od myšlenky k realizaci [3]. Ta definuje marketingovou komunikaci jako souhrn veškerých komerčních i nekomerčních komunikačních nástrojů, které jsou využívány k podpoře či dosažení marketingové strategie organizace.

Ve výsledku se tedy v případě marketingové komunikace nejedná o pouhou komunikaci se zákazníky a snahu ovlivnit jejich chování a postoje, nýbrž tento pojem zahrnuje i například komunikaci s akcionáři, zaměstnanci, dodavateli apod. Lze tedy rozlišovat firemní komunikaci a marketingovou tržní komunikaci. Ačkoliv tyto složky nelze striktně oddělovat, neboť se navzájem prolínají, budu se v praktické části té-to práce soustředit především na marketingovou tržní komunikaci směrem k zákazníkovi.

Přestože je komunikace v marketingu často chápána jako masová záležitost, existují výjimky, jako je například osobní prodej či přímá komunikace. V minulosti se využívala právě primárně komunikace hromadná, nicméně s postupujícím časem, a především pak vývojem komunikační techniky a narůstající individualizaci vztahů, se tato rovnováha poněkud pozměnila a přímé komunikaci se přikládá postupně stále větší význam.

2.6.2 Historie

Marketingová komunikace má svou historii a vývoj. Od vystavování zboží a vyvolávačů na tržištích se posunula díky rozvoji technologií a zdokonalování reklamních prostředků do podoby, kdy marketingová komunikace neznamená jen reklamu, nýbrž ucelený komplexní nástroj. [4]

Pro ilustraci uvádím stručný přehled významných mezníků ve vývoji marketingové komunikace (převzato z [7]). Každý z nich významně ovlivnil směr, kterým se marketingová komunikace ve svém dalším vývoji dále ubírala:

- 400 př. n. l. – Vyvolávači v antickém Řecku
- 1477 – První reklama v Anglii
- 1655 – Ustanovení užívání slova „advertising (propagace)“
- 1871 – První známý výzkum efektivity reklamy (A Guide to Advertising)
- 1926 – První komerční rádio (USA)

- 1947 – První komerční televize (USA)
- 1971 – Vynalezení prvního emailu
- 1991 – První webové stránky, 2G bezdrátová telefonní technologie
- 1998 – Založení společnosti Google
- 2005 – Založení společnosti Facebook

V následující části budu čerpat převážně z [7], neboť obsahuje poměrně podrobnou historii vývoje tohoto fenoménu. Ač někteří možná až přehnaně spekulují, zdali se nedá za úplně nejstarší formu marketingové komunikace či propagace považovat umění pravěkých nástěnných maleb či desatero biblických přikázání, je nesporným faktem, že prvopočátky je možné v té nejzákladnější formě najít třeba už ve starověkém Babyloně. Tehdy se jednalo primárně o speciální rozlišující značky různých řemeslníků, což by se dnes dalo označit jako způsob brand marketingu.

Pokud zůstaneme ve starověku, tak Řekové krom značek disponovali i funkcí tzv. vyvolávačů. Jejich primární účel byla hlasitá hlasová propagace zákonů, nicméně dali se najímat i obchodníky k lepšímu zviditelnění jejich výrobků či služeb, což by se dnes označilo za podporu prodeje (sale promotion). Do časů Říma se koncept vyvolávačů široce rozšířil a pevně usadil v kultuře. Další důkazy o existenci nových forem propagace byly nalezeny například v Pompejích, které byly po výbuchu sopky velmi dobře zakonzervovány. Zde krom již zmíněných značek obchodníků se nacházely „reklamní“ nápisy na zdech.

Během středověku se příliš mnoho nezměnilo, stále se držely vyvolávači a značky jako formy komunikace, a to až do doby vynálezu knihtisku v roce 1447. To byl první výrazný zlom pro tehdejší podobu marketingové komunikace, neboť s sebou přinesl mnoho nových možností, jako např. snazší výroba, větší objem výroby atd. Rozmáhá se tvorba plakátů a nejvýraznějším faktorem, který ovlivnil směr vývoje marketingové komunikace, byl rozvoj novinového tisku. Velice brzy se totiž zjistilo, že za drobné místo pro propagaci obchodníci rádi zaplatí, čímž se dobře částečně pokryjí náklady na tisk a výrobu novin. Noviny se tedy zakrátko staly vedoucím způsobem pro jakoukoliv propagaci služeb či výrobků.

Klíčovým obdobím pro nastartování skutečného rozvoje základů moderní marketingové komunikace a propagace vůbec byla industriální revoluce. Tehdy došlo k posunu od lokálních malovýrob k velkovýrobám v továrnách a rozvinuly se i nové a lepší distribuční cesty po širokém

okolí (např. železnice). Výrobky se mohly dostávat i do vzdálených měst, kde bylo ale třeba lidi o nich informovat a to vedlo k vyššímu soustředění se právě na marketingovou komunikaci.

V polovině 19. století pak došlo k rozdělení pojmů, označení „reklama“ zůstalo vyhrazeno pouze na placenou masmediální komunikaci, a nikoliv pro celkovou oblast marketingové komunikace. Postupem času a vývoje převzaly dominantní úlohu médií rádia a televizní stanice. Největší rozvoj propagačního odvětví nastává pak ve druhé a třetí čtvrtině 20. století a dochází k rozvoji i dalších marketingových komunikačních nástrojů.

Zatím posledním velkým zlomem v rozvoji marketingové komunikace byla na konci 20. století takzvaná „digitální revoluce“. Příchod internetu, emailu a později vznik webových vyhledávačů a sociálních sítí otřásl s dosavadním pojetím marketingové komunikace a otevřel jí mnoho nových dveří. Neznamenalo to ovšem, že předcházející média byla zapomenuta, naopak rádio či televize se velmi efektivně integrovaly s novými možnostmi. Digitalizace především velmi výrazně zpřístupnila informace a přinesla mnoho nových způsobů, jak např. se zákazníky komunikovat.

Lze říci, že marketingová komunikace je v neustálém pohybu a pružně se mění. Reaguje nejen na technologické vývoje, ale i na změny hodnot společnosti. Nemůže se zastavit a musí neustále sledovat své okolí, aby mohla správně cílit a oslovovat své cílové objekty. Technologické pokroky umožňují stále nové a lepší možnosti marketingové komunikace, nicméně nelze opomínat lidský faktor kreativity a schopnost dostat ty správné informace ke správným lidem ve správný čas.

Jak již bylo naznačeno, k samotné reklamě a prezentaci se postupně přidávaly další a další aktivity, které měly určitý společný cíl. Na původně samostatné aspekty a formy komunikace se postupně začalo nahlížet jako na soubor souvisejících aktivit. Přestalo se jednat pouze o čistý součet přínosů jednotlivých aktivit, ale zvýšil se zájem o jejich vzájemnou integraci a výsledný synergický efekt, který vytvářely vzájemným doplňováním se a podporou.

V dnešní době již nelze marketingovou komunikaci provádět neorganizovaně a vytrženě z okolního kontextu. A právě funkční vzájemně interaktivní působení jednotlivých aktivit marketingové komunikace, včetně jejich synergického efektu dalo vzniknout na přelomu 20. a 21. století teorii integrované marketingové komunikace. Integrovanou marketingovou komunikací tedy rozumíme optimální spojení nejrůznějších forem dostupných nástrojů marketingové komunikace tak, aby v konkrétní situaci měly co největší požadovaný účinek.

Současně v této době dochází i ke vzniku a zdokonalování nových metod marketingové komunikace (např. guerilla marketing či marketing sociální). [4]

Ještě v roce 2012 uvádí [4], že se ve světe jemně odlišovalo to, co všechno pod pojem marketingová komunikace spadá. V jistých publikacích byla marketingová komunikace brána jako ekvivalentní označení pro celou složku „promotion" v marketingovém mixu, jinde bylo marketingovou komunikací chápáno integrované působení všech součástí propagačního mixu (promotion mix). Z toho lze vyvodit, že je tento pojem stále živý a dochází k jeho průběžnému upřesňování, sjednocování a přesnějšímu vymezování.

2.6.3 Dělení marketingové komunikace

Marketingová komunikace je nejběžněji členěna na nadlinkové aktivity a podlinkové aktivity [4]. Za nadlinkové aktivity se považuje propagace tak, jak si ji většina lidí představuje, tedy televizní a rozhlasová reklama, využití billboardů, tisku atd. Podlinkovou komunikací se potom míní například podpora prodeje, osobní prodej, přímý marketing (direct marketing), vztahy s veřejností (public relations) atd.

Existuje mnoho nástrojů různě pracujících s komunikací. Cílem dobré komunikační strategie je zvolit takové, které v souhrnu a správném poměru dobře poslouží našemu záměru. Nástroje představené níže představují výčet základních možností, které bude možné v praktické části využít pro návrh efektivní marketingové komunikace pro zvolený typ správy sítě.

Zdroje [6] a [3], ze kterých budu v následující kapitole nejvíce čerpat, například rozdělují nástroje marketingové komunikace přibližně stejně na „staré a tradiční" a „mladé a moderní". Rozhodně to však není jediné možné dělení.

Autorka v [6] uvádí, že toto dělení vyhovuje potřebám malých a středních firmem a není vyloučené dělení jiným způsobem, neboť neexistuje přesně dané obecné rozdělení. Pod tato rozdělení pak konkrétně uvádí jednotlivé nástroje. [15] většinu zmíněných „mladých a nových" nástrojů označuje za nástroje progresivního marketingu.

Staré a tradiční

- Reklama
- Podpora prodeje
- Vztahy s veřejností
- Osobní prodej
- Přímý marketing

Mladé a nové

- Buzz marketing (virální marketing, WOM, guerillový marketing)
- Obsahový marketing

V tomto dělení je zohledněno, že v dnešní době se reklama vyskytuje jak v offline podobě jako plakáty, letáky apod., ale že velká část se přesunula i do formy onlinové, například na sociálních, sítích jako je facebook. Pro většinu zmíněných platí, že se nevyskytuje v ryze jediné podobě, ale že se mohou vyskytovat jak v offline, tak online podobě.

2.6.4 Nástroje marketingové komunikace

Marketingová komunikace má nepřeberné množství nástrojů a vzhledem k tomu, že se stále poměrně aktivně vyvíjí a adaptuje na změny, i repertoár jejích nástrojů se aktualizuje a obměňuje. Vyjmenovat je všechny není předmětem této práce, a proto zde bude uvedeno jen pár nejvýraznějších či nejvíce používaných.

2.6.4.1 Reklama

Jde o nejvíce výraznou formu reklamy, která je často laiky považována za rovný ekvivalent marketingové komunikace. Z finančního hlediska se zpravidla jedná o nejnákladnější položku. Příkladem formy reklamy je například inzerce v tisku, televizní a rozhlasové spoty, venkovní reklama (billboardy či plakáty), letáky či reklama v kinech. [6] uvádí, že v dnešní době se na tuto plošnou reklamu pohlíží poněkud s nedůvěrou. Běžný člověk z ní dostává pocit, že propagovaný produkt bude v sobě mít nějaký háček.

2.6.4.2 Podpora prodeje

[6] charakterizuje podporu prodeje jako souhrn veškerých aktivit, které přímo vedou k posílení prodeje. Často se váže ke konkrétnímu místu a jejím cílem je prudké krátkodobé navýšení prodeje, bez dlouhodobějšího udržení tohoto nárůstu. Nevede k dlouhodobější loajalitě zákazníků. Tento nástroj je nejvíce využívám při zavádění výrobku či služby na trh, výprodejích atd. Do tohoto druhu marketingové komunikace lze zapojit i partnery a dodavatele a společně pak působit na cílovou skupinu. Takovouto spolupráci označujeme jako společnou podporu prodeje. Bývá efektivní, nicméně současně velmi náročná na organizaci a komunikaci. Konkrétním příkladem podpory prodeje, jsou například slevové akce, výstavy a veletrhy, podpůrné akce v místě prodeje či různé soutěže a hry.

2.6.4.3 Vztahy s veřejností (Public relations)

Dle [6] je tento komunikační nástroj využíván především pro budování dobrého jména firmy, produktu či služby. Tento nástroj umožňuje šířit propagační aktivitu a v určitých situacích lze jeho vhodným využíváním zabránit špatnému obrazu firmy, produktu či služby pro zákazníky. Aktivity v rámci vztahů s veřejností nemají nic nabízet ani prodávat. Skutečným cílem je poskytovat relevantní informace pro konkrétní zájem veřejnosti (cílové skupiny). Jedná se o zákaznicky velmi populární nástroj, je velmi sledovaný.

Už bylo řečeno dříve, že veřejnost nebo „zákazník“ nemusí být nutně pouze koncový spotřební zákazník. I zde platí, že za veřejností mohou být například zaměstnanci, vláda (goverment relations), média (press relations), investoři, partneři v odvětví a tak dále [6] (viz Obrázek č. 8). Pro každou takovou skupinu se pak využívá odlišný přístup v rámci vztahů s veřejností a poskytují se jim právě takové informace, které jsou pro ně nejvíce relevantní.

Obrázek 8 - Vztahy s veřejností a jejich formy [17]

Vztahy s veřejností mohou být jak v online, tak offline podobě a následně uvádím příklady různých běžných forem, které se v rámci vztahů s veřejností využívají [6]:

- Tiskové publikace – výroční zprávy, brožurky pro zákazníky, atd.
- Veřejné akce – přednášky, veletrhy, akce pro veřejnost/zaměstnance, atd.
- Firemní identita (Corporate Identity, CI) – logo, písmo, barevnost, vizitky, atd.
- Projekty sociální zodpovědnosti (CSR).

Projekty sociální zodpovědnosti jsou ta část vztahů s veřejností, pomocí které je možnost propojit firmu, produkt nebo službu s některým z neziskových témat, např. šetrnost k životnímu prostředí. Na tato témata a spojení je všeobecně společností velmi příznivě nahlíženo a často jsou i mediálně zajímavá a mluví se o nich. Jedná se o vylepšování jména firmy, produktu či služby, nikoliv přímo o prodejní aktivitu. Taktéž se nejedná o něco s okamžitým efektem, ten se projeví v dlouhodobém a budovaném časovém horizontu. Troufám si tvrdit, že speciálně v současnosti, kdy se čím dál více lidí zajímá například o to, z čeho a jakým způsobem jsou výrobky vytvářeny, hrají projekty sociální zodpovědnosti nemalou roli v tom, jak jsou výsledné výrobky vnímány.

2.6.4.4 Osobní prodej

Jedná se dle [6] o samotný prodej přímo konkrétnímu zákazníkovi či zákazníkům za pomoci přímého osobního kontaktu. Silnou stránkou tohoto nástroje je například vysoká úspěšnost, lepší komunikace a zpětná vazba přímo od zákazníka. Slabou stránkou a potenciální nevýhodou je pak menší záběr a vyšší náklady, které plynou z individuálního přístupu. Osobní prodej najde uplatnění jak na B2B tak B2C trhu. Příkladem osobního prodeje je pak například budování vztahů se současnými zákazníky, CRM systém (Customer relationship system) a podobně.

2.6.4.5 Přímý marketing

Podobně jako osobní marketing je přímý marketing individuálně cílený, nicméně se v tomto případě jedná o zpravidla masovější záležitost bez osobního kontaktu a povětšinou psanou formou – často pomocí hromadných nástrojů jako pošta či email. Cílem je vytvořit elektivní databázi zákazníků. Příkladem přímého marketingu může být email, SMS, poštovní zásilky, katalogy a podobně. [6]

Při takovýchto marketingových aktivitách je třeba brát v potaz omezení a nařízení vyplývající z tzv. Antispamového zákona (Zákon č. 480/2004 Sb. [14]), na jehož dodržování dohlíží Úřad pro ochranu osobních údajů. Tento zákon upravuje mimo jiné zodpovědnost poskytovatelů za to, jak nakládat s daty, které poskytne uživatel, s daty, které se dočasně ukládají, nebo například to, za jakých podmínek lze šířit obchodní sdělení. Plné znění a podrobnosti jsou uvedeny v [14].

2.6.4.6 Buzz marketing

Buzz marketing je druh marketingu, který se opírá o vyvolání rozruchu a zájmu. Cílem je, aby se po prvotních impulzech rozproudila živá debata mezi lidmi – ideálně pak cílovou skupinou, tedy zákazníky. I informace o produktu či službách se nadále má šířit samovolně díky aktivitě a debatám samotných lidí. [6] vyjadřuje také myšlenku, že tento nástroj vyžaduje hodně energie, kreativity a nadšení. Především je to však dobrý nápad, kterým firma přitáhne onu prvotní pozornost a podnítí další diskuzi mezi lidmi.

Osobně vidím velké využití Buzz marketingu skrze internet, a to ať už se jedná o internetové diskuze zaměřené na hodnocení služeb či produktů, sociální sítě, které ať se nám to líbí, nebo ne dokáží šířit některé informace bleskovou rychlostí, nebo třeba webové stránky zaměřené na video, jako například youtube.

Úskalím, se kterým je u buzz marketingu nutno počítat je fakt, že pokud usiluje firma o vyvolání rozruchu, může se uchýlit ke kontroverzním či nezvyklým nápadům. U takovýchto nápadů existuje vždy riziko, že impuls bude přijat negativně.

Buzz marketing se může vyskytovat v různých formách a podobách. Mezi nejznámější z nich patří [6]:

Virální marketing

Již zmíněná prezentace online pomocí textu, videa, obrázku či dokumentu. Možností šíření je například email nebo sociální sítě, kde se šíří především díky dobrovolnému sdílení nebo pomocí takzvaných hashtagů, které umožňují snadno vyhledávat další příspěvky označené daným konkrétním hashtagem.

Dobré slovo (Word of mouth, WOM)

Jedná se o šíření informací a případně zkušeností s produktem či službou mezi lidmi. Často se jedná o recenzi, doporučení či osobní zkušenost. WOM může být jak pozitivní, tak negativní povahy a může se šířit jak po internetu, tak mimo něj.

Guerillový marketing (Guerrila marketing)

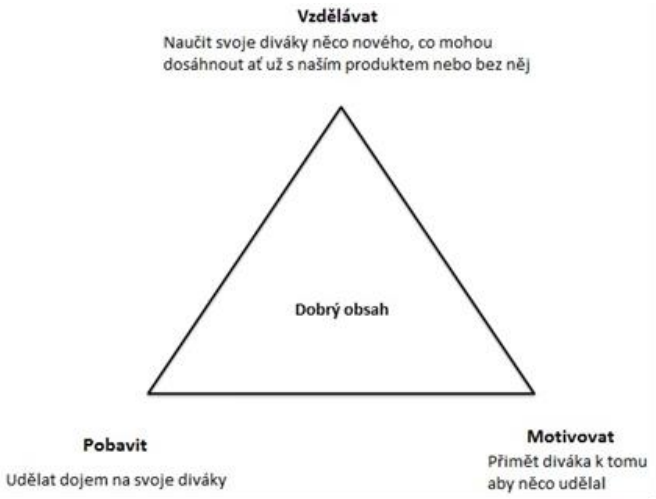
Cílem tohoto druhu marketingu je s pomocí co nejnižší investice peněz do-sáhnout co nejlepší propagace. [15] Guerillový marketing vznikl v 70. letech 20. století a byl inovativní především právě tím, že představoval marketingový nástroj vyžadující minimum peněžní investice. Charakteristickým rysem tohoto nástroje je nečekaná, drastická, krátkodobá, humorná, levná kampaň. Existuje více typů guerrilového marketingu a některé z nich se pohybují na samé hranici zákona a slušnosti. Příkladem takového marketingu může například nošení a distribuce triček s tištěným názvem a adresou konkrétní webové stránky, kterou chceme propagovat.

2.6.5 Obsahový marketing (Content marketing)

Jedná se o jeden z novějších/mladších marketingových nástrojů, který využívá užitečný či důležitý obsah, který by mohl přitáhnout další potenciální zákazníky zajímající se o danou oblast. Myšlenkou je dobrým obsahem zaujmout budoucí i stávající zákazníky, vtáhnout je do komunikace a posléze nechat tento obsah se podvědomě šířit. Obecně můžeme říct, že ideálním cílem je ovlivnění a zlepšení chování spotřebitele [15].

Obsahový marketing se soustředí na tvorbu vlastního obsahu a médií. Takovýto obsah není snadné vytvořit a měl by pokud možno splňovat tři základní podmínky – vzdělávat, pobavit, motivovat (viz. Obrázek č. 9 [15]). Jinými slovy cílem není propagovat a prodávat produkt firmy, nýbrž poskytovat zdarma cílové skupině vzdělávací a poučné informace.

Content marketing je bohužel dlouhodobý nástroj a jeho výsledky se neprojeví hned, nýbrž až s větším odstupem času. Taktéž vyžaduje velký vklad investované práce, a to v pravidelném, nikoliv jednorázovém intervalu. [6]



Obrázek 9 - Obsahový marketing - složení dobrého obsahu (Content marketing) [15]

3 Praktická část

Prvním cílem této praktické části je na základě informací získaných v teoretické části porovnat oba představené modely správy sítí, kontrolerový model správy sítě a cloudový model správy sítě a určit předpokládanou pozici těchto dvou modelů na trhu správy sítí v blízké budoucnosti

Druhým cílem této praktické části je provést segmentaci trhu zabývající se správou sítí, určit relevantní kritéria pro jeho segmentaci, zhodnotit jejich význam v rámci této konkrétní segmentace, určit významné segmenty trhu. Pro tyto segmenty bude posléze jednotlivě provedeno vyhodnocení a určení, který ze dvou představených alternativ představených v této práci, naplňuje potřeby a požadavky lépe.

V závěru práce se potom pro jeden ze zvolených přístupů ke správy sítě na základě určených cílových segmentů trhu vytvoří model vhodné marketingové komunikace za použití nástrojů představených v úvodní teoretické části. Úplným závěrem potom bude krátké ekonomické porovnání diskutovaných variant.

3.1 Srovnání modelů typu kontroler a typu cloud

V kapitolách 2.3. a 2.4. byly představeny dva přístupy k správě sítí – kontrolerový a cloudový. Rozhodně nelze říci, že by jedno či druhé řešení bylo všeobecně lepší a správné a vytlačilo v dohledné době svého konkurenta z trhu. Oba modely mají své silné i slabé body a pro každý z nich se stále najde vhodné využití a cílová skupina zákazníků, pro které je nejlepším řešením. Během práce bylo zmíněno mnoho vlastností pro oba typy modelů, v této kapitole se je pokusím shrnout a vzájemně přehledně porovnat ve dvou tabulkách.

Kromě logický variant silná – slabá stránka, jsem se rozhodla do přehledové a hodnotící tabulky připojit ještě třetí sloupec „Neutrální“. Tento sloupec bude sloužit pro buďto neutrální vlastnosti daného modelu, nebo pro atributy, které nejsou jednoznačné a mohou být jak výhodou, tak nevýhodou, záleží na okolnostech a kontextu.

Silné stránky	Neutrální	Slabé stránky
Platí se pouze to, co zákazník využívá	Odpovědnost za zabezpečení dat/komunikace leží u poskytovatele	Omezená customizace
Jednodušší přístup k prvkům skrze jednotný nástroj	Využitelné ve firmách i domácnostech	Nutnost internetového připojení
Nový moderní přístup – cloud je na vzestupu		Náchylné na pasivní sí'tové útoky
Snadno škálovatelný		Jistá závislost na funkčnosti služeb třetí strany
		Pravidelné většinou roční poplatky za službu

Tabulka 1 - Přehled silných a slabých stránek modelu správy sítě typu cloud

Silné stránky	Neutrální	Slabé stránky
Velká customizace	Využitelné ve firmách i domácnostech	Často nevyužité či nedostačující zdroje
Osvědčená metodika		Odpovědnost za zabezpečení komunikace a aktualizace leží u zákazníka
Není ve správě třetí strany (nemá závislost na její funkčnost)		Zdlouhavé připojování se jednotlivě na prvky sítě
		Náchylnější k vážnějším dopadům při lidské chybě

Tabulka 2 - Přehled silných a slabých stránek modelu správy sítě typu kontroler

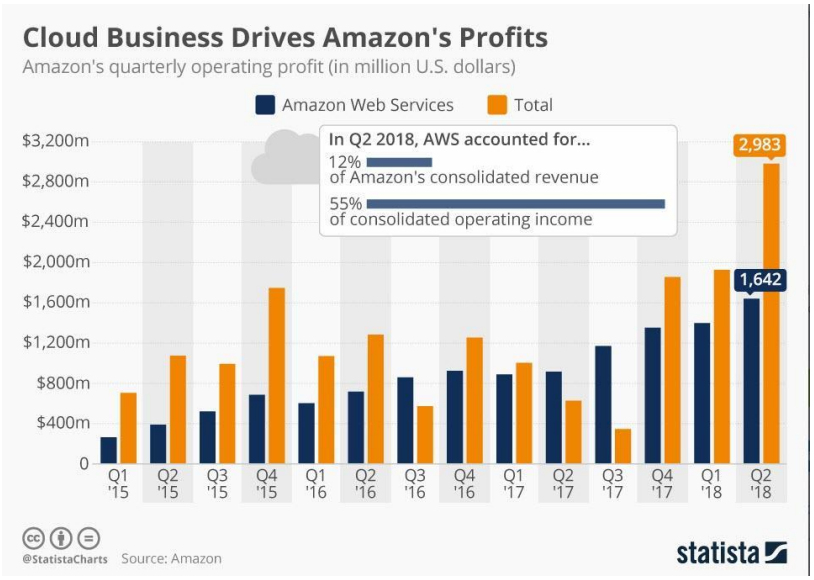
Jak je z tabulek jasně patrné, v některých případech se stává, že silná stránka jednoho z modelů je slabou stránkou pro ten druhý jako například otázka uživatelské customizace (silná stránka kontroleru) nebo jednoduchosti při přístupu ke správě jednotlivých prvků (silná stránka cloudu). V jiných otázkách jsou si oba přístupy relativně rovny např. vhodnost pro domácnost i firmu. I když zde musím připustit, že i když jsem uvedla tuto vlastnost jako neutrální, nemůžu popírat fakt, že cloudové řešení je o trochu vhodnější pro firemní prostředí a kontroler pro jednoduché ploché sítě domácností.

3.2 Předpokládaná budoucí pozice jednotlivých modelů správy sítí

V této části se pokusím sumarizovat a popsat předpokládaný vývoj trhu. Vycházet budu především z postoje ke cloudovým řešením obecně, jejichž součástí jsou bezesporu i cloudové přístupy ke správám sítí. Jako podklady pro následující závěry jsem vyhledala a prošla několik různých statistických zhodnocení, závěrů a predikcí pro následující roky, z nichž jako nejrelevantnější byly vybrány [23] a [24] z důvodu značné šíře informací a důvěryhodnosti. Právě ty poskytly výchozí bod a oporu pro závěry učiněné v této kapitole.

Lze říci, že v současné době se nacházíme v situaci, kdy je přijímání cloudových řešeních (ať už jakéhokoliv druhu) relativně v počátcích. Podle některých zdrojů pouhá desetina pracovní zátěže, která by na cloud mohla být přenesena, skutečně přenesena byla. Nicméně o cloudových řešeních se stále častěji mluví a diskutuje.

Ať je stav přijetí cloudových řešení v současnosti jakýkoliv, už teď se jedná o segment trhu, který generuje biliony dolarů v ročních příjmech, a nezdá se, že by ten-to trend měl v nejbližší době zpomalovat. Příkladem budiž jedna z největších cloudově zainteresovaných společností Amazon Web Services (AWS), které cloudový business v druhém čtvrtletí roku 2018 vydělal 55 % celkového provozního zisku (Obrázek č. 10).



Obrázek 10 - Zisk z cloudového businessu AMW za druhé čtvrtletí roku 2018 [24]

Meziroční růst popularity a využití cloudových řešení je krásně vidět na statistice firmy Ganter ze září roku 2018 (viz. Obrázek č. 11), která zobrazuje predikci celosvětových příjmů veřejných cloudových služeb v miliardách amerických dolarů až do roku 2021. V tabulce jsou názorně rozlišeny i jednotlivé modely cloudových řešení SaaS, PaaS a IaaS. Pro tuto práci jsou především zajímavé hodnoty pro SaaS.

Table 1. Worldwide Public Cloud Service Revenue Forecast (Billions of U.S. Dollars)

	2017	2018	2019	2020	2021
Cloud Business Process Services (BPaaS)	42.2	46.6	50.3	54.1	58.1
Cloud Application Infrastructure Services (PaaS)	11.9	15.2	18.8	23.0	27.7
Cloud Application Services (SaaS)	58.8	72.2	85.1	98.9	113.1
Cloud Management and Security Services	8.7	10.7	12.5	14.4	16.3
Cloud System Infrastructure Services (IaaS)	23.6	31.0	39.5	49.9	63.0
Total Market	**145.3**	**175.8**	**206.2**	**240.3**	**278.3**

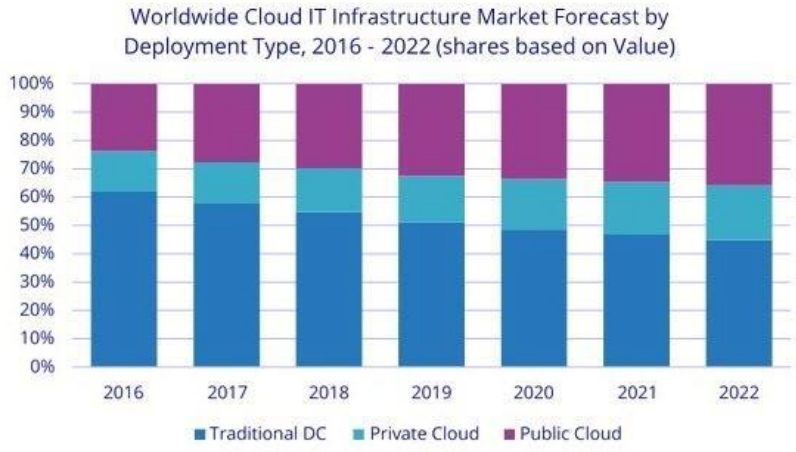
BPaaS = business process as a service; IaaS = infrastructure as a service; PaaS = platform as a service; SaaS = software as a service
Note: Totals may not add up due to rounding.

Source: Gartner (September 2018)

Obrázek 11 - Predikce celosvětových příjmů veřejných cloudových služeb [24]

Z výše zmíněných skutečností lze celkem s jistotou vyvozovat, že cloudová řešení, včetně cloudového přístupu ke správě sítí, s největší pravděpodobností neoslabí svou pozici na trhu, spíše naopak. Naopak díky vzestupu cloudových řešení budou tradiční možnosti jako fyzický hardware a kontrolerová řešení pro správu sítí na své pozici poněkud oslabovat, alespoň co se týče firemních prostředí. V kontextu fyzických osob a běžných domácností se nepředpokládá tak markantní posun, neboť pro jejich potřeby povětšinou postačuje jediný router – jejich sítě jsou jednoduché a ploché. Pro ně by cloudová řešení správy nepřinášela zdaleka tak výrazný rozdíl a pravděpodobně by si pouze připlatili.

O narůstající popularitě a lukrativnosti cloudových řešeních svědčí například i to, kolik prostředků se skutečně do zdrojů pro provoz a rozvoj těchto služeb investuje. V současnosti se odhaduje přibližně 10,9 % meziroční růst celkových nákladů na IT infrastrukturu pro nasazení cloudových prostředí. Předpokládá se, že za současných podmínek by do roku 2022 výdaje na cloudové infrastruktury měly přesáhnout výdaje vynaložené na necloudové IT infrastruktury (viz. Obrázek 12).



Obrázek 12 - Předpověď vývoje celosvětové cloudové IT infrastruktury [24]

Už bylo zmíněno dříve, že odborníci v horizontu příštích až deseti letech předpokládají další rapidní vývoj a posílení pozice cloudových řešení na úkor zpomalujících se tradičních alternativ. Samotný trh veřejných cloudových služeb (public cloud services market) v letošním roce vzrostl o 21 % a pro příští rok společnost Ganter předpokládá meziroční růst o 17,33 %,

přičemž nejrychleji rostoucím segmentem trhu by pak měl být IaaS. I přesto by si svou pozici nejvýznamnějšího segmentu měl zachovat SaaS, do kterého spadá i námi zkoumaná cloudová správa sítí.

Z toho, co bylo uvedeno v této kapitole, lze vyvodit poměrně jasný závěr, že cloudová řešení nejen ve správě sítí jsou důstojným konkurentem klasickým kontrolerovým/fyzickým modelům, a předpokládám, že na své pozici budou minimálně v příštích pěti letech nadále posilovat až do stavu, kdy se podíl trhu se pro obě varianty vyrovná, či dokonce mírně nakloní ve prospěch cloudových řešení.

3.3 Stanovení cílových skupin

Tato podkapitola se bude zabývat volbou a definicí vhodných kritérií pro segmentaci trhu zákazníků, stanovením jejich priorit a samotnou segmentací trhu do jednotlivých dostatečně heterogenních skupin. V závěru kapitoly se potom pokusím určit, který, popřípadě které ze segmentů zákazníků jsou pro jednotlivé modely správy sítí, které jsem popsala v kapitolách 2.2. a 2.3., nejvhodnější na zacílení.

3.3.1 Stanovení kritérií pro segmentaci trhu uživatelů

Základem pro správnou segmentaci uživatelů je vhodné určení jednotlivých kritérií segmentace, a to tak, aby tato kritéria byla jak významná z hlediska zájmového cíle, a tak současně vytvořila dostatečně vnitřně homogenní skupiny zákazníků, kteří se ovšem dostatečně výrazně od sebe odlišují svým nákupním chováním na trhu. Pro tyto skupiny vytvořím modelové označení a sadu atributů jasně charakterizující daný segment. Segmentačních kritérií existuje nepřeberné množství a je pod-statné zvolit nejenom ta správná a relevantní, ale i jejich vhodné množství. Segmentační kritéria jsem volila v závislosti na znalostech nabytých v teoretické části práce.

V následujících podkapitolách budou mnou zvolená segmentační kritéria pro trh správy sítí vyjmenována a podrobněji popsána. Tabulky číslo 3, 4 a 5 sumarizují všechna zvažovaná významná kritéria pro segmentaci. Některá kritéria segmentace navazují na kritérium „charakter subjektu“ z první tabulky, které je nejvýznamnějším kritériem z hlediska prvotní segmentace,

a vztahují se pouze k jedné části trhu. V tabulce jsou uvedeny i jednotlivé varianty očekávaných relevantních možností v rámci kritéria.

Kritérium	Varianta 1	Varianta 2
Charakter cílového subjektu	Firma	Fyzická osoba

Tabulka 3 - Primární segmentační kritérium

Kritérium	Varianta 1	Varianta 2
Věk	18 – 40 let	Více jak 40 let
Zaměření na IT	Vlastní odborné vzdělání ze střední odborné nebo vysoké školy	Nevlastní odborné vzdělání ze střední odborné nebo vysoké školy
Finanční možnosti	Dobré	Průměrné

Tabulka 4 - Sekundární segmentační kritéria pro Fyzickou osobu

Kritérium	Varianta 1	Varianta 2	Varianta 3	Varianta 4
Zaměření na IT	Firma podniká v IT	Firma nepodniká v IT		
Rozsáhlost firmy	Mikropodnik	Malý podnik	Střední podnik	Velký podnik
Charakter firmy	Soukromá	Státní		
Finanční možnosti	Dobré	Průměrné		
Vyžadovaná SLA				

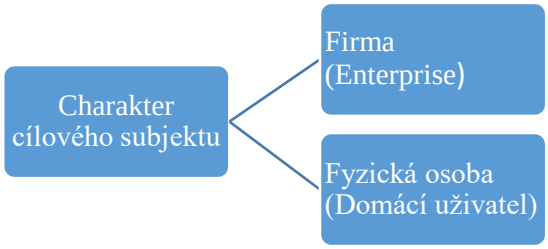
Tabulka 5 - Sekundární segmentační kritéria pro Firmy

3.3.1.1 Charakter cílového subjektu

Charakterem cílového subjektu se rozumí určení, zda se jedná o jednotlivce (běžného člověka, domácí uživatele), nebo o firmu. Tento aspekt výrazně ovlivňuje nákupní chování potenciálních zákazníků a taktéž dle něj lze poměrně značně diverzifikovat vhodný způsob marketingové komunikace. Vhodné přístupy pro komunikaci s firmou či jedincem se totiž dost výrazně liší.

Ze závěrů vyplývajících z teoretické části práce lze usuzovat, že pro tento konkrétní případ bude pravděpodobnějším typickým zákazníkem spíše firma než jednotlivec, neboť firmy a větší instituce často disponují rozsáhlými propojenými sítěmi zařízení, které je třeba odpovědně a pravidelně spravovat.

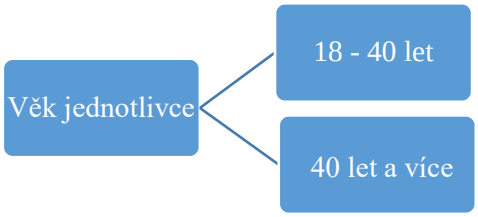
Nicméně čím více elektronických zařízení napojených do sítě se v našich domácnostech objevuje, tím více roste potřeba správy sítí i v běžných domácnostech. Proto se domnívám, že je třeba důkladně prozkoumat i možnosti a příležitosti mimo čistě firemní trh.



Obrázek 13 - Popis kritéria "Charakter cílového subjektu"

3.3.1.2 Věk

Věk představuje segmentační kritérium relevantní pro nadsegment domácích uživatelů a jedná se o jedno z nejběžnějších demografických kritérií u potenciálních zákazníků. V různém věku mají lidé jiné potřeby a jiné motivace. Je běžné z hlediska věku segmentovat podměrně podrobně do mnoha skupin, nicméně pro tento konkrétní případ jsem se rozhodla použít pouze dvě následující skupiny.



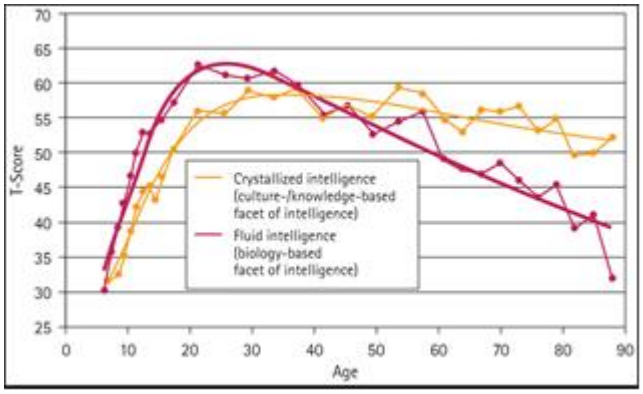
Obrázek 14 - Popis kritéria "Věk"

Důvodem pro zvolení mezního věku 40 let je zamýšlená účel tohoto segmentačního kritéria. Je patrné, že s postupně narůstajícím věkem se často vytrácí ochota lidí zkoušet nové a modernější možnosti či zařízení (v tomto případě se jedná o v současnosti stále relativně nový cloudový přístup ke správě sítí). Mladí lidé mají větší predispozice k tomu být otevření inovacím a novým možnostem především v oblastech IT, tudíž jsou i pravděpodobnějším zákazníkem/potenciálním zájemcem o relativní novinky a inovace. U starších lidí se potom mnohem častěji setkáváme s neochotou opustit fungující a osvědčené přístupy, metody, produkty či služby.

Věkové kategorie byly nastaveny s následujícím odůvodněním. Do 18 let jsou mladí lidé z valné většiny nevýdělečně činní a sdílí domácnosti se svými rodiči, kteří by v takové domácnosti byli nositeli finálního rozhodnutí o případné metodě správy sítě.

Mezní věk 40 let pro přechod z inovativně pozitivního k inovativně zdrženlivému přístupu jsem zvolila na základě studií o vývoji lidské inteligence, která úzce souvisí se schopností a predispozicemi učit se a přijímat nové věci. [21] a [22] rozděluje lidskou inteligenci na fluidní (fluid intelligence) a krystalickou (crystallized inteli-gence). Fluidní inteligence představuje tu část inteligence, která je nezávislá na kulturním prostředí a učení a odpovídá za učení se novým věcem. Krystalická inteligence pak čerpá z již naučených informací a životních zkušeností. Jak popisují články [21] a [22] a jak je ukázáno na Obrázku č. 14, v průměru přibližně kolem 40 roku života se postavení inteligencí obrátí a dominantním se stává spoléhání se na zkušenosti.

Nutno ovšem připustit, že IT je velice rychle se vyvíjející oblast a je pravděpodobné, že věk, kdy se lidé posouvají od ochoty/schopnosti se neustále sebevzdělávat a zkoušet nové alternativy řešení (ať už správy sítí, či jiné), bude o něco vyšší než obecně v populaci.



Obrázek 15 - Vývoj lidské inteligence v průběhu života [21]

T-Score je standardizované skóre umožňující porovnání hodnot mezi různými měřeními. Převzato z [21], kde rovněž podrobněji popsáno.

3.3.1.3 Zaměření na IT

Společné kritérium jak pro jednotlivce, tak pro firmy je kritérium specializace v oboru IT.

U firem je jím myšleno to, že podnikají v oboru a zaměstnávají větší či menší počet specialistů na správu sítí, a je tedy větší pravděpodobnost, že mají buď vlastní interně vedený a spravovaný systém správy sítí, nebo specifické a náročné požadavky na takový systém, často s požadavkem na dobrou uživatelskou customizaci (přizpůsobení na míru) jejich potřebám, kterou by cloudové řešení nemuselo vždy uspokojit.

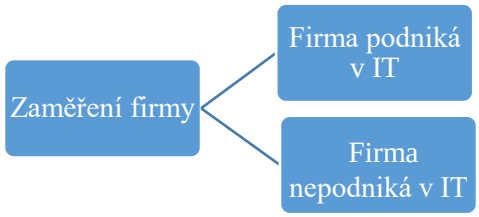
Výjimkou jsou pak společnosti, které se přímo zaměřují na správy prostředí svých zákazníků. Ty by pravděpodobně mohly cloudové řešení docenit, neboť by se jim výrazně usnadnila práce (minimálně z časového hlediska), pokud by mohli všechny sítě spravovat z jediného nástroje dostupného odkudkoliv.

Naopak firmy nezabývající se primárně IT sice mívají taktéž interní IT oddělení, ale jsou otevřenější co největšímu zjednodušení a spokojí se s menší mírou na-stavitelných možností pro správy sítě, pokud to poslouží jejím účelům.

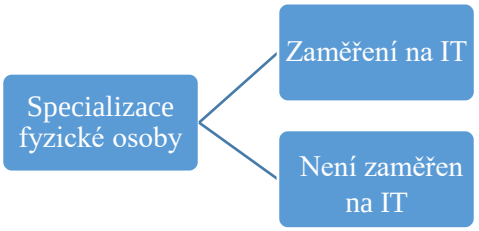
Pro jednotlivce považuji za zaměření na IT povolání v tomto oboru nebo vystudování některé z oborově zaměřených škol – střední odborné školy, vysoké školy, atd. V oboru se pohybující osoby jsou otevřenější alternativám a novinkám, především ve stále dynamicky

se vyvíjejícím IT, nicméně o to více technických specifikací a podrobných informací vyžadují. Do této kategorie by se dali zařadit i lidé, pro které je IT koníčkem a jsou nadšenci. Takoví lidé mají tendenci zajímat se o novinky v IT, sledovat je a často si je i sami v improvizovaném domácím prostředí zkoušet.

Pro fyzické osoby nepracující v oboru ani se nezajímající o IT nebude mít cloudové řešení správy sítí přílišný užitek ani zajímavost.



Obrázek 16 - Popis kritéria "Zaměření na IT" pro firmy



Obrázek 17 - Popis kritéria "Zaměření na IT" pro fyzické osoby

3.3.1.4 Rozsáhlost firmy

Jako další z poměrně význačných segmentačních kritérií pro firmy jsem zvolila jejich rozsáhlost. Toto kritérium by mělo zohledňovat aspekty jako velikost firmy, počet poboček, geografické rozmístění poboček (zdali jsou např. od sebe navzájem v dojezdových vzdálenostech), počet stálých zaměstnanců atd. Všechny tyto aspekty se odrazí na komplexnosti sítí minimálně pro vnitřní infrastrukturu firmy.

Velikost podniků definuji podle dělení dle pravidel Evropské unie [25], jak ilustruje tabulka č. 6, kde jeho primárním faktorem dělení je počet zaměstnanců a roční obrat nebo bilanční suma roční rozvahy.

Velikost firmy	Počet zaměstnanců	Roční obrat/bilanční suma roční rozvahy v milionech EUR
Mikropodniky	Méně než 10	Do 2
Malé podniky	10 – 50	2 - 10
Střední podniky	50 – 250	10 – 43
Velké podniky	Nad 250	Nad 43

Tabulka 6 - Popis kritéria "Rozsáhlost firmy"

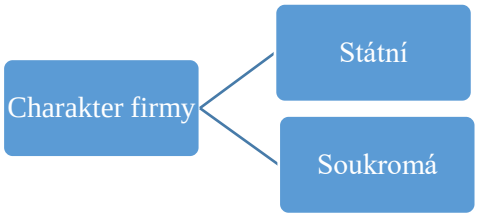
Různá velikost se odlišně promítne do potřeb pro správu sítí. Mikropodniky jsou natolik malé, že lze předpokládat relativně plochou síť, kterou nebude příliš obtížné a časově náročné spravovat. Pro tento typ firmy by mohl stále být přijatelnější kontrolerový přístup.

U malých a středních podniků už se může objevit zájem o jednoduše použitelný nástroj – cloudový nástroj – pro správu sítí. Těmto podnikům nebude vadit omezená přizpůsobitelnost nástroje, a naopak by uvítali jednoduchý nástroj pro údržbu, o který by se nemuseli starat, neboť provoz, údržba a aktualizace budou v rukou poskytovatele (viz kapitola 2.4.2.). Mnoho malých firem v průzkumech uvádělo, že jejich obecný zájem o cloudová řešení je motivován právě tím, že se o správu samotného nástroje nebudou muset starat samy či prostřednictvím externího specialisty, který jim buď chybí, či je třeba jeho schopnosti a čas využít na jiné úkoly.

Pro velké firmy by naopak cloudový přístup správy mohl být velmi vhodným zjednodušením práce. Takovéto firmy mají často více geograficky vzdálených poboček a nesídlí v jedné kanceláři či patře a sítě i jen uvnitř samotné organizace rostou do komplexních celků.

3.3.1.5 Charakter firmy

Další vhodným kritériem pro rozdělení trhu firem nejen v IT je pak i její charakter - zdali se jedná o státní, nebo soukromou společnost. Státní společnosti mají daná pravidla a povinnosti, které musí dodržovat (např. o vedení veřejných zakázek a výběrových řízení), často jsou svazovány i dalšími omezeními. Prosadit se s alternativním přístupem či najít přijatelnou cenovou rovnováhu pro obě strany může být proto značně náročnější než v soukromých firmách, které tak striktním pravidlům nepodléhají. Současně státní podniky mohou dávat přednost vlastním řešením z důvodu obavy o bezpečnost dat a informací.



Obrázek 18 - Popis kritéria "Charakter firmy"

3.3.1.6 Finanční možnosti zákazníků

V tomto případě ne zcela zásadním, nicméně neopomenutelným kritériem jsou samozřejmě finanční možnosti zákazníka. Velké firmy mají jiné finanční možnosti než malé firmy a jednotlivci. Pronajímat si cloudový nástroj na správu sítí nemusí být pro jednotlivce a malé firmy finančně výhodné, neboť skutečná přidaná hodnota tohoto nástroje – dostupnost odkudkoliv a přístup ke všem sítím z jednoho místa – se plně projeví až s větším počtem spravovaných sítí, které pro tyto subjekty nejsou příliš typické.

3.3.1.7 Vyžadovaná firemní SLA

Opět se jedná o doplňkové kritérium pro tento konkrétní případ. Pokud pracujeme s jakýmkoliv nástrojem v IT, speciálně pak pokud se jeho užití týká firem podnikajících v oboru, je vždy nutno zvážit nebo se minimálně zamyslet nad tím, jaké SLA (Service-level agreement) je přípustné pro daný problém, v tomto případě závadu na síti a její opravu.

Je zásadní rozdíl, pokud se problém vyskytne na spravované síti zákazníka, kde hrozí penále za příliš dlouhou nefunkční službu, nebo pokud se pokazí prvek v síti v domácí firmě na personálním oddělení. Druhý případ sice také bude nepříjemný, ale pravděpodobně výrazněji nepoškodí firmu.

3.3.2 Stanovení důležitosti a priorit jednotlivých kritérií

Při segmentaci trhu a hledání vhodných cílových segmentů se téměř nelze vyhnout většímu množství segmentačních kritérií. Pro lepší zacílení a výsledky je následně vhodné si určit, která kritéria jsou z hlediska dané problematiky významnější.

Pro tuto práci jsem kritéria z kapitoly 3.3.1 rozdělila do dvou podskupin a to na „Významná kritéria“ a „Doplňková kritéria“ viz Tabulka 7 a 8, které popisují významná a doplňková kritéria pro firmy a fyzické osoby zvlášť. Při tomto dělení byly zohledňovány očekávané segmentační charakteristiky jednotlivých kritérií z kapitoly 3.3.1 a míra jejich dopadu při dělení trhu potencionálních zákazníků na menší segmenty.

Významné kritérium	Doplňkové kritérium
Charakter cílového subjektu	Charakter firmy
Rozsáhlost firmy	Finanční možnosti
Zaměření na IT	Vyžadovaná SLA

Tabulka 7 - Přehled významnosti jednotlivých kritérií pro firmy

Významné kritérium	Doplňkové kritérium
Charakter cílového subjektu	Finanční možnosti
Věk (fyzické osoby)	Vyžadovaná SLA
Zaměření na IT	

Tabulka 8 - Přehled významnosti jednotlivých kritérií pro fyzické osoby

3.3.3 Segmentace trhu – určení a definice skupin uživatelů

Na základě kritérií definovaných v kapitole 3.3.1., se zohledněním jejich významností, které jsem popsala v kapitole 3.3.2. a se znalostmi načerpanými v teoretické části, jsem určila následující významné modelové segmenty trhu správy sítí. Při volbě segmentů jsem se snažila pokrýt co největší možnou variabilitu možností potencionálních zákazníků, nicméně přitom stále držet rozumnou generičnost, protože je nesmyslné tvořit segmenty o jednom potenciální zákazníkovi a celý proces segmentace pozbývá na významu. Definované segmenty jsou následující:

Fyzická osoba A

Jedná se fyzickou osobu ve věku do 40 let, s profesním zaměřením či zájmem o IT. Člověk, spadající do tohoto segmentu nebude nutně pro svůj běžný život potřebovat nejnovější novinky, které se objeví. Jeho kupní motivací bude zájem inovace starých způsobů a možnost vyzkoušet si něco nového, speciálně, pokud je daná věc IT komunitou dobře přijímána.

Fyzická osoba B

Jedná se o fyzickou osobu ve věku nad 40 let, pohybující se profesně v prostředí IT. Osoba reprezentující tento segment taktéž nepotřebuje pro svůj běžný život novinky v podobě cloudových správ sítí. O novinkách si rád přečte, aby se udržel profesně v obraze, nicméně pokud nebude muset, sám je zkoušet nebude.

Firma A

Jedná se o středně velkou soukromou firmu, podnikající v IT. Firma A o trendy a novinky v IT zajímá. Disponuje středně rozsáhlou firemní síť a určitý počet specialistů, kteří mají kromě údržby sítě pravděpodobně ještě jiné povinnosti. Firma A má potřebu stabilní a funkční sítě s co nejmenšími starostmi. Jednoduchá, ale efektivní řešení zaujmou její pozornost.

Firma B

Jedná se o soukromou firmu velké velikost, jejíž předmět podnikání nesouvisí s oborem IT. Firma B se příliš o trendy a novinky v IT nezajímá. Disponuje rozsáhnou a komplexní sítí

rozdělenou geograficky do více míst, což vyžaduje více specialistů na různých místech. Firma B hledá nástroj, který jí správu sítí ulehčí.

Firma C

Jedná se o soukromý mikropodnik, podnikající v sektoru IT a s požadavky na přísná SLA. Firma C je velice malý podnik s jednoduchou plochou sítí. O novinky v IT se zajímá a volnému vyzkoušení nástrojů neřekne ne, ale pro své užití hledá nekomplikované a především levné řešení. Ve své velikosti nemá Firma C potřebu složitých programů a funkcí pro správu své sítě.

Firma D

Jedná se o středně velký státní podnik, nepodnikající v IT s omezenými finančními možnostmi. Firma D se o novinky v IT příliš nezajímá. Disponuje středně velkou sítí a velice se zajímá o otázky bezpečnosti. Firma D by mohla mít motivaci pro nové modely správy sítí, ale její finanční možnosti jsou limitované a musí i v tomto případě čelit doporučením a limitacím i z jiných směrů než čistě správa IT.

Firma E

Jedná se o soukromou firmu malé velikosti, která nepodniká v oboru IT, a nejsou na ní kladeny požadavky na přísná SLA, které by mohly být ne-funkčností sítě ovlivněny. Firma E se nezajímá příliš o novinky v IT a disponuje malou interní sítí. Na její správu zaměstnává specialistu. Občasné komplikace na síti jsou nepříjemné, ale nikoliv likvidační. Tato firma sama aktivně nové možnosti správ sítě nevyhledává, nicméně je ani neodmítá.

3.3.4 Určení cílových skupin pro jednotlivé typy modelů správy

V kapitole 3.3.3. jsem na základě segmentačních kritérií a jejich stanovených priorit určila celkem sedm významných segmentů trhu. Jedná se jak o fyzické osoby, tak o firmy. Každý ze segmentů má poněkud odlišné motivace a nákupní chování. Dle jejich potřeb, zájmů a motivací uvedených v kapitole 3.3.3., lze přiřadit ke každému segmentu model síťové správy, který by jeho potřebám nebo zájmům více vyhovoval. Pro přehled uvedeno v následující tabulce.

Segment trhu	Přiřazený nástroj správy sítě
Fyzická osoba A	Cloudový typ
Fyzická osoba B	Kontrolerový typ
Firma A	Cloudový typ
Firma B	Cloudový typ
Firma C	Kontrolerový typ
Firma D	Kontrolerový typ
Firma E	Cloudový typ

Tabulka 9 - Přehled přiřazení modelu správy sítě k segmentům trhu

3.4 Návrh vhodné marketingové komunikace pro variantu cloudového řešení

Pro návrh vhodné marketingové strategie jsem si vybrala cloudové řešení pro správu sítí. Pro své rozhodnutí jsem měla hned několik důvodů. Zaprvé cloudový přístup je poměrně nový a vzhledem k prognóze růstu jeho pozice na trhu má i potenciál získat dobré budoucí postavení. Současně se domnívám, že se o něm příliš nehovoří, a tudíž je zde velký prostor pro vytvoření efektivní a účinné kampaně.

Při tvorbě návrhu se bude vycházet z následujících skutečností. Tvořit se bude marketingová komunikace pro cloudový přístup ke správě sítí. Díky kapitole 3.3.4. jsou známy cílové segmenty (Tabulka č.10). Je znám nejsilnější konkurent na trhu, tj. model kontrolerové správy sítí. A také je dostupná informace, že přestože není cloudový přístup nejsilnějším hráčem na trhu, neustále posiluje svou pozici a předpokládá se, že v tom bude minimálně ve světě pokračovat.

Cílový segment1	Cílový segment 2	Cílový segment 3	Cílový segment 4
Fyzická osoba A	Firma A	Firma B	Firma E

Tabulka 10 - Přehled cílových segmentů pro návrh marketingové komunikace

Krom informací, které jsou známy, jsou ovšem i takové, které známy nejsou. Konkrétně nemní stanovený žádný konkrétní časový úsek, po který má navržená komunikace probíhat, neznáme totožnost a možnosti objednatele marketingové komunikace a ani rámcový rozpočet, na kampaň. Díky tomu je tento návrh omezen o fakt, že není možné provést vnitřní analýzu a není možné určit silné a slabé body podniku, který by tuto marketingovou komunikaci žádal.

Za takovýchto podmínek bude návrh čistě teoretický a primárně se bude zaměřovat na výběr vhodných marketingových nástrojů a jejich kombinace bez ohledu na celkové výdaje.

Z představených nástrojů marketingové komunikace budeme cílit především na ty vhodné pro firmy vzhledem k tomu, že ve třech ze čtyřech cílových segmentů se jedná o společnost. V takovém případě například klasická reklama a většina čistě mass mediálních nástrojů nebude příliš vhodná.

Pro tvorbu komunikačního plánu existuje nejedno doporučení, podle kterého je možno postupovat. Slečna Formánková [36] ve své diplomové práci uvádí převzaté dva hlavní, dle Pelsmackera a dle Korlera. Pelsmacrekova varianta tvoří marketingovou komunikaci hledáním odpovědí na následující otázky: [36]

- Analýza situace a marketingové cíle. Proč?
- Určení cílové skupiny. Kdo?
- Stanovení komunikačních cílů. Co?
- Výběr nástrojů, technik, kanálů a médií. Jak a kde?
- Stanovení rozpočtu. Kolik?
- Měření výsledků. Jak efektivně?

Naproti tomu Kotler netvoří marketingovou komunikaci hledáním odpovědí, ale následováním čtyř základních poučení a to: [36]

- Určení cílového publika a komunikačních cílů.
- Připravit sdělení.
- Vybrat média.
- Zajistit zpětnou vazbu nutnou k měření účinků komunikace.

Pro tento případ, kdy nejsme schopni odpovědně určit vnitřní analýzu situace, dám přednost následování doporučení Kotlera pro tvorbu této marketingové komunikace pro cloudový přístup ke správě sítí.

3.4.1 Určení cílového publika a komunikačních cílů

Cílové publikum máme díky provedené segmentaci v kapitole 3.3. již jasné. Jedná se o Fyzickou osobu A a Firmy A,B a E (viz Tabulka č. 10). Soustředila bych se především primárně na oslovení firem a Fyzickou osobu bych ponechala jako doplňkovou cílovku. Nedá se totiž předpokládat, že fyzická osoba by přinesla tak velký ať už přímý nebo nepřímý zisk/užitek v rámci tohoto případu.

Co se týče komunikačních cílů, pro tento případ navýšení povědomí o existenci cloudového modelu správy sítí o např. 15 % a mírné navýšení stálých zákazníků (např. o 5 %). Je vždy třeba výt v určování cílů konkrétní, neboť to pak umožní na celou marketingovou komunikaci vyhodnotit a určit zda byla úspěšná či nikoliv.

3.4.2 Vybrat média

Vzhledem ke komunikačnímu cíli určeném ve 3.4.1. se vhodné nástroje budou pravděpodobně nacházet ve druhém, třetím nebo šestém sloupci.

	Zvýšení prodeje	Zvýšení povědomí o značce	Ovlivňování postojů ke značce	Zvýšení loajality ke značce	Stimulace chování směřujících k prodeji	Budování trhu
Reklama		XXX	XXX			XXX
Direct marketing	XXX			XXX	XXX	
Podpora prodeje	XXX				XXX	XXX
Public relations		XXX	XXX			XXX
Event marketing			XXX	XXX		
Sponzoring		XXX	XXX			
Osobní prodej	XXX			XXX	XXX	
On-line komunikace	XXX	XXX	XXX		XXX	

Tabulka 11 - Nejvýznamnější funkce jednotlivých marketingových nástrojů [36]

Jelikož se jedná hlavně o firmy v této cílové skupině, volila bych více zacílené nástroje jako direct marketing a online komunikaci, např. emailovou komunikaci. Samozřejmě veřejné akce nejsou od věci v podobě účasti na technickém veletrhu nebo konferenci, kde je možnost oslovit více lidí naráz a převážně odborníky z dalších firem.

Co bych nerada opomněla při volbě komunikačních nástrojů je buzz marketing, konkrétně jeho podskupina Word of mouth. Speciálně v odvětví IT a v rámci jednotlivců funguje Word of mout výborně. Sousta specialistů se mezi sebou navzájem zná a rádi mezi sebou sdílí novinky a názory na ně. Pro ještě větší podpoření Word of mouth může být využito například youtube kanálů od recenzentů

3.4.3 Zajistit zpětnou vazbu nutnou k měření účinků komunikace

Hodnocení nejen marketingových komunikací nikdy nebude jednotné a potvrzuje to i [36]. V našem případě je vyhodnocení nemožné, neboť nemáme s čím porovnávat, ale protože jsme si zvolili za cíl něco měřitelného – míra povědomí a počet stálých dotazníků, pravděpodobně by byl vytvořen dotazník, který by byl zaslán vybrané skupině respondentů (pravděpodobně mix zákazníků a nezákazníků) a náležitě vyhodnocen.

3.5 Ekonomické porovnání modelů z pohledu koncového uživatele

Všechny faktické informace použité pro tuto kapitolu byly převzaty z teoretické části práce, primárně kapitol 2.3. a 2.4. .

Pro krátké ekonomické porovnání budeme zvažovat tři varianty, které budou zohledňovat i prvotní investice na související zařízení.

- Kontrolerová varianta správy na vlastním hardwaru.
- Cloudová varianta správy na vlastním hardwaru.
- Cloudová varianta správy na cloudově pronajímaném hardwaru.

První dvě zmíněné varianty jsou varianty, které byly definovány a používány pro účely této práce. Poslední variantu jsem přidala jako zajímavou alternativu, která by v budoucnu, s navyšujícím se zájmem o cloud a jeho využívání, mohla stát přijatelnou alternativou i pro některé cílové skupiny, pro které byla v současně diskutované podobě cloudová varianta nevýhodná či zbytečná. V této části předpokládám, že zákazník by variantu správy sítí volil pro svoje interní firemní či domácí použití, nikoliv jako nástroj pro výkon svého předmětu podnikání, tedy správy sítí svých vlastních klientů.

Každá z těchto variant má lehce odlišnou strukturu výdajů jak iniciálních, tak provozních. Varianta kontrolerové správy má vysokou položku počátečních investic do zařízení a během svého provozu vyžaduje odborníka pro svou správu. Počet potřebných odborníků k bezproblémovému fungování sítě záleží na její velikosti a komplexnosti. Tento počet poroste rychleji než stejná potřeba u zbylých dvou variant.

Varianta cloudové správy na vlastním hardwaru podobně jako předchozí varianta zahrnuje velkou počáteční investici do zařízení. K této položce přibude pravidelný, pravděpodobně roční poplatek za cloudové nástroje pro management sítí. I zde bude přítomna položka za IT specialistu, ale bude nižší než v případě kontrolerového typu a bude růst jiným tempem, neboť pomocí cloudového nástroje pro správu sítě bude specialista schopen snáze a rychleji spravovat i složitější sítě, a to bez potíží a omezení i na větší vzdálenost.

Poslední varianta cloudové správy na cloudovém hardwaru nezahrnuje žádnou prvotní investici a po celou dobu užívání bude pouze zákazník platit dva poplatky, jeden za cloudovou správu sítě a druhý za cloudový hardware a najaté specialisty ve stejné míře jako v předchozí variantě. Pro úplnou přehlednost jsem tyto skutečnosti shrnula v následující tabulce.

Varianta	Prvotní investice	Výdaje na specialisty	Poplatek za cloudový nástroj správy sítě	Poplatek za cloudový hardware
Kontroler + HW	Ano	Větší	Ne	Ne
Cloud + HW	Ano	Nižší	Ano	Ne
Cloud + Cloud HW	Ne	Nižší	Ano	Ano

Tabulka 12 - Přehled výdajů spojených s jednotlivými modely správy sítě

Lze konstatovat, že výsledné rozhodnutí, která z variant se ekonomicky více vyplatí, bude záležet na velikosti konkrétní firmy a její sítě a také na délce plánovaného využívání daného řešení. V krátkodobějších horizontech by se s největší pravděpodobnosti vyplatila varianta třetí, pokud bychom uvažovali horizont v řádu let, mohlo by se ukázat, že nejvýhodnějším řešením bude u průměrně velké sítě kontrolerový přístup, který má po svém zavedení relativně nízké provozní náklady. Na co by se také nemělo při vyhodnocení zapomenout, je skutečnost, že po

určitém počtu let bude nutné dosloužilý HW obměnit za nový, což také ovlivní celkové zhodnocení.

4 Závěr

Cílem této práce bylo seznámit se dvěma alternativními způsoby správy sítí a pro jeden z nich vytvořit návrh vhodné marketingové komunikace.

V první části práce jsem shrnula a popsala, co sítě jsou a jaký mají význam pro každodenní život moderního člověka. Následoval stručný popis základních síťových prvků a jejich účelu a představila jsem i oba modely správy sítě včetně jejich silných a slabých stránek. Zvláštní kapitola byla věnována i bezpečnosti sítí a důkladně byly popsány především dopady síťových útoků na cloudové řešení, které může být náchylné nejen na pasivní síťové útoky.

Posledním bodem teoretické části potom bylo objasnění pojmu marketingová komunikace. Společně s definicí tohoto stále se dynamicky vyvíjejícího odvětví jsem přidala stručnou historii a přehled základních komunikačních nástrojů rozdělených na tradiční, jako např. reklama či noviny, a nové. Tyto nástroje byly potom využity jako množina možností pro návrh marketingové komunikace pro cloudovou správu sítí.

V praktické části jsem se nejprve věnovala vzájemným porovnáním obou představených typů a přehledně popsala silné i slabé stránky, které byly zmiňovány v teoretické části. Nelze jednoznačně říct, že by jeden z modelů správy sítě byl lepší než ten druhý. Vhodnost řešení silně závisí na cílové skupině, neboť je nutné zohlednit faktory jako charakter cílové skupiny (zdali se jedná o firmu či jednotlivce), rozsáhlost firmy, finanční možnosti, atd. V současnosti stále existují cílové skupiny jako mikropodniky, pro které je lepším řešením kontrolerový model, ale i takové, pro které je jednoznačně výhodnější řešení cloudové jako velké decentralizované firmy s rozsáhlou interní sítí. Bylo provedeno i zhodnocení současné a předpokládané pozice jednotlivých přístupu v blízké budoucnosti. Podle závěrů, k nimž jsem na základě studia analýz v rámci podkapitoly 3.2. dospěla, lze předpokládat že cloudová řešení obecně budou na trhu v příštích letech posilovat.

Poslední velký celek mé práce se zabýval stanovením návrhu vhodné marketingové komunikace pro zvolený přístup ke správě. S ohledem na poznatky načerpané v teoretické části jsem určila vhodná kritéria dělení trhu a jejich významnost. Na základě těchto kritérií (např. věk u fyzických osob nebo velikost a za-měření u firem) pak byly definovány významné tržní segmenty, které byly následně přiřazeny k jednotlivým správám sítě dle toho, které řešení bylo pro daný segment trhu vhodnější. Toto určení jednotlivých segmentů trhu potvrdilo dříve stanovenou tezi, že v současnosti je na trhu místo pro obě tato řešení.

Přínos své práce vnímám v komplexním shrnutí obou typů správy sítí, zvláště pak cloudového, který by při současném vývoji mohl dle poznatků popsaných v kapitole 4.2. v budoucnu minimálně ve firemním sektoru zaujmout významnou pozic, zvláště pak ve větších firmách a ve firmách, kde je nutné spravovat geograficky roztříštěné sítě (ať už z důvodu různě umístěných poboček či zaměření na správu sítí jiných subjektů). Další přínos potom vidím v podrobné segmentaci trhu od stanovení vhodných kritérií, přes jejich význam pro šetření až po určení cílových segmentů.

Možnost budoucího rozšíření této práce vidím například v přesnějším ohodnocení jednotlivých segmentačních kritérií. Rozdělení na „Významná“ a „Doplň-ková“ pro základní určení stačí, ale pro přesnější výsledky by zřejmě bylo vhodné zvážit možnost váženého ohodnocení jednotlivých kritérií, které by po-mohlo zohlednit i relativní míru různosti důležitosti jednotlivých kritérií.

Taktéž vhledem k všeobecné rostoucí popularitě cloudových řešení a zájmu o ně vidím i mnoho příležitostí pro budoucí zlepšení navrhovaného marketingového marketingové komunikace, neboť s tím, jak se bude jeho postavení na trhu a v podvědomí zákazníků měnit, bude třeba i náležitě upravit či změnit používané nástroje. V neposlední řadě jako prostor pro další zlepšení a prohloubení práce se nabízí možnost rozšířit část obsahující ekonomické zhodnocení variant o konkrétní finanční vyčíslení pro jednotlivé varianty pro konkrétní podnik či fyzickou osobu.

5 Seznam použitých zkratek

Zkratka	Anglický název	Český název
CNC	Cloud Networking Center	Cloudové sítové centrum
DDoS	Distributed Debial of Service	Rozptýlené odmítnutí služby
DoS	Denial of Service	Odmítnutí služby
HW	Hardware	Fyzické IT zařízení
IaaS	Infrastructure as a Service	Infrastruktura jako služba
ISO	International Organization for Standardization	Mezinárodní organizace pro standardy
IT	Information Technology	Informační technologie
LAN	Local Area Network	Lokální síť
MITM	Man in the Middle	Útok typu „muž uprostřed“
OSI model	Open Systems Interconnection Model	Referenční ISO/OSI model
PaaS	Platform as a Service	Platforma jako služba
SaaS	Software as a Service	Software jako služba
SLA	Service level Agreement	Smlouva na úrovni služeb
WAN	Wide Area Network	Rozlehlá síť

Tabulka 13 - Seznam použitých zkratek

6 Seznam použitých obrázků

7 Seznam použitých tabulek

8 Seznam použitých zdrojů

[1] White Paper: Network management - who needs it?. ComputerWeekly.com | Information Technology (IT) News, UK IT Jobs, Industry News [online]. Dostupné z: http://www.computerweekly.com/feature/White-Paper-Network-management-who-needs-it

[2] Network management. In: AbriaCloud Technologies [online]. 2018 [cit. 2018-03-13]. Dostupné z: https://abria.cloud/net-management

[3] TOMEK, Gustav a Věra VÁVROVÁ. Marketing od myšlenky k realizaci. 3. aktualizované doplněné vydání. Praha: Professional publishing, 2011. ISBN 987-80-7431-042-3.

[4] JURÁČKOVÁ, Olga a Pavel HORŇÁK. Velký slovník marketingových komunikací. Praha: Grada, 2012. ISBN 97-80-247-4354-7.

[5] Marketingový mix [online]. In: . [cit. 2018-03-27]. Dostupné z: http://mujsvetmarketingu.cz/wp-content/uploads/2017/04/graf.png

[6] ECKHARDTOVÁ, Jana. 7 nejčastějších nástrojů marketingové komunikace. In: Malá marketingová [online]. [cit. 2019-01-08]. Dostupné z: http://www.malamarketingova.cz/komunikacnimix.html

[7] EGAN, John. Marketing communications. Second edition. London: Sage, 2015. ISBN 978-1-4462-5902-3.

[8] Security Issues and Computer Network Management [online]. In: . [cit. 2018-05-01]. Dostupné z: https://insights.speakwithageek.com/post/Security-Issues-and-Computer-Network-Management-1

[9] Computer networking. In: Nibusinessinfo [online]. [cit. 2018-05-01]. Dostupné z: https://www.nibusinessinfo.co.uk/content/network-security-issues

[10] IT risk management. In: Nibusinessinfo [online]. [cit. 2018-05-01]. Dostupné z: https://www.nibusinessinfo.co.uk/content/it-risk-assessment-methodology

[11] Protect your business online. In: Nibusinessinfo [online]. [cit. 2018-05-01]. Dostupné z: https://www.nibusinessinfo.co.uk/content/server-security

[12] Network Management System: Best Practices White Paper. In: Cisco [online]. [cit. 2018-05-01]. Dostupné z: https://www.cisco.com/c/en/us/support/docs/availability/high-availability/15114-NMS-bestpractice.html

[13] Cloud Computing. In: Nibusinessinfo [online]. [cit. 2018-05-01]. Dostupné z: https://www.nibusinessinfo.co.uk/content/cloud-computing

[14] Zákon č. 480/2004 Sb., o některých službách informační společnosti ve znění účinném od 1. července 2017. Úřad pro ochranu osobních údajů [online]. [cit. 2018-05-22]. Dostupné z: https://www.uoou.cz/zakon-c-480-2004-sb-o-nekterych-sluzbach-informacni-spolecnosti/ds-1497/archiv=1&p1=2317

[15] VANĚK, Petr. Marketingové aspekty webových stránek. Liberec, 2017. Diplomová práce. Technická univerzita v Liberci.

[16] Cloud Network Center [online]. In:.[cit. 2018-05-22]. Dostupné z: https://www.zyxel.com/cz/cs/products_services/Cloud-Network-Center-CNC/application-diagram

[17] Public relations. In: SketchBubble [online]. [cit. 2018-05-22]. Dostupné z: https://www.sketchbubble.com/en/powerpoint-public-relations.html

[18] Cloud service models. In: Uniprint.net [online]. [cit. 2018-05-22]. Dostupné z: https://www.uniprint.net/wp-content/uploads/2017/05/Cloud-service-models-diagram.png

[19] Man in the middle attack. In: Incapsula [online]. [cit. 2018-05-22]. Dostupné z: https://www.incapsula.com/images/illustrations/web-app-security-mini-site/man-in-the-middle-mitm.jpg

[20] VANĚK, Petr. Man in the middle útoky: Semestrální práce. In: . 2014.

[21] VOELKLE, Manuel C. a Ulman LINDENBERGER. Cognitive Development. In: Frontiers for young minds [online]. 24. 4. 2014 [cit. 2019-01-08]. Dostupné z: https://kids.frontiersin.org/article/10.3389/frym.2014.00001#table-1

[22] FORREST, Conner. SaaS, PaaS, and IaaS: Understand the differences. In: ZDNet [online]. 1. 11. 2017 [cit. 2019-01-08]. Dostupné z: https://www.zdnet.com/article/saas-paas-and-iaas-understand-the-differences/

[23] Cloud Computing - Statistics & Facts. In: Statista: The Statistics portal [online]. [cit. 2019-01-08]. Dostupné z: https://www.statista.com/topics/1695/cloud-computing/

[24] COLUMBUS, Louis. Roundup Of Cloud Computing Forecasts And Market Estimates, 2018. Forbes [online]. 23. 9. 2018 [cit. 2019-01-08]. Dostupné z: https://www.forbes.com/sites/louiscolumbus/2018/09/23/roundup-of-cloud-computing-forecasts-and-market-estimates-2018/#7708a5d5507b

[25] Pomůcka pro určení velikosti podniku. Operační program Praha - Adaptibilita: Praha & EU Investujeme do vaší budoucnosti [online]. 30. 12. 2009 [cit. 2019-01-08]. Dostupné z: http://prahafondy.ami.cz/cz/oppa/pro-prijemce/325_pomucka-pro-urceni-velikosti-podniku.html

[26] FORREST, Conner. SaaS, PaaS, and IaaS: Understand the differences. In: ZDNet [online]. 1. 11. 2017 [cit. 2019-01-08]. Dostupné z: https://www.zdnet.com/article/saas-

paas-and-iaas-understand-the-differences/

[27] Monitoring and Managing Networks in the Cloud. Zyxel [online]. srpen 2015 [cit. 2019-01-08]. Dostupné z: ftp://ftp.zyxel.com/Cloud_Network_Center/datasheet/Cloud%20Network%20Center_1.pdf

[28] Pasivní síťové prvky (Passive Networking Components). Management mania [online]. 29. 1. 2018 [cit. 2019-01-08]. Dostupné z: https://managementmania.com/cs/pasivni-sitove-prvky

[29] Aktivní síťové prvky (Active Networking Hardware). Management mania [online]. 31. 1. 2017 [cit. 2019-01-08]. Dostupné z: https://managementmania.com/cs/aktivni-sitove-prvky

[30] Počítačové siete [online]. [cit. 2019-01-08]. Dostupné z: http://upol.jecool.net/sk/8-zakladni-sitove-prvky/

[31] The Difference Between a Router, Switch and Hub. Webopedia: Online Tech Dictionary for Students, Educators and IT Professionals [online]. 27. 10. 2017 [cit. 2019-01-08]. Dostupné z: https://www.webopedia.com/DidYouKnow/Hardware_Software/router_switch_hub.asp

[32] Router (Směrovač). Management mania [online]. 14. 9. 2018 [cit. 2019-01-08]. Dostupné z: https://managementmania.com/cs/smerovac-router

[33] Access point (AP), přístupový bod. Management mania [online]. 26. 11. 2017 [cit. 2019-01-08]. Dostupné z: https://managementmania.com/cs/access-point-ap-pristupovy-bod

[34] Network management. In: Progressive: Experience outcomes [online]. [cit. 2019-01-08]. Dostupné z: https://progressive.in/wp-content/uploads/2018/01/newtwork-

manag.png

[35] PAWAR, Mohan V. a J. ANURADHAB. Network Security and Types of Attacks in Network [online]. In: . Procedia Computer Science Journal, 2015 [cit. 2019-01-08]. Dostupné z: https://www.sciencedirect.com/science/article/pii/S1877050915006353

[36] FORMÁNKOVÁ, Lucie. Tvorba komunikační kampaně. Brno, 2012. Diplomová práce. Masarykova univerzita Ekonomicko-správní fakulta. Vedoucí práce Ing. Klára Kssparová.

A Obsah přiloženého DVD

Přiložené DVD obsahuje kompletní práci v souboru ve formátu pdf a zadání práce ve větším rozlišení ve formátu pdf.

Obsah DVD:

- Zadani_diplomova_prace_Ulrichova_2019.pdf – soubor se zadáním diplomové práce v PDF formátu
- Diplomova_prace_Ulrichova_2019.pdf – soubor s vlastním textem práce v PDF formátu