VYSOKÁ ŠKOLA POLYTECHNICKÁ JIHLAVA

Katedra cestovního ruchu

Kybernetická bezpečnost pro podnikání v kyberprostoru v oblasti cestovního ruchu

bakalářská práce

Autor práce: Jana Franková

Vedoucí práce: Ing. Dagmar Frendlovská, Ph.D.

Jihlava 2019

Vysoká škola polytechnická Jihlava

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Autor práce:	**Jana Franková**
Studijní program:	Ekonomika a management
Obor:	Cestovní ruch
Název práce:	**Kybernetická bezpečnost pro podnikání v kyberprostoru v oblasti cestovního ruchu**
Cíl práce:	Cílem bakalářské práce je představit čtenářům možnosti bezpečného kybernetického podnikání v oblasti cestovního ruchu. Práce je rozdělena na teoretickou a praktickou část. Teoretická část se věnuje podobám podnikání v kyberprostoru v oblasti cestovního ruchu, dále základním pojmům jako jsou: kyberprostor, kybernetická bezpečnost pro podnikání, remailary, darknets, atd. Praktická část analyzuje situaci, předkládá přednosti a rizika podnikání v kyberprostoru. Cílem dotazníkového šetření je zjistit s jakými nástrahami se podnikatelé ve virtuálním prostředí potýkají a jak je řeší. Přínosem bakalářské práce je návrh možností pro bezpečné podnikání v kyberprostoru.

Ing. Dagmar Frendlovská, Ph.D.
vedoucí bakalářské práce

RNDr. Eva Janoušková, Ph.D.
vedoucí katedry
Katedra cestovního ruchu

Abstrakt

Cílem bakalářské práce je představit čtenářům možnosti bezpečného kybernetického podnikání v oblasti cestovního ruchu. Práce je rozdělena na teoretickou a praktickou část. Teoretická část se věnuje podobám podnikání v kyberprostoru v oblasti cestovního ruchu, dále základním pojmům jako jsou: kyberprostor, kybernetická bezpečnost pro podnikání, remailary, darknets, atd. Praktická část analyzuje situaci, předkládá přednosti a rizika podnikání v kyberprostoru. Cílem dotazníkového šetření je zjistit s jakými nástrahami se podnikatelé ve virtuálním prostředí potýkají a jak je řeší. Přínosem bakalářské práce je návrh možností pro bezpečné podnikání v kyberprostoru.

Klíčová slova

Podnikání, kyberprostor, kybernetická bezpečnost, hrozby/nástrahy virtuálního světa.

Abstract

The aim of the bachelor thesis is to introduce to the readers the possibility of safe cyber business in the field of tourism. The thesis is divided into the theoretical and practical part. The theoretical part deals with forms of cyberspace business in the field of tourism, basic terms such as cyberspace, cyber security for business, remailers, darknets, etc. The practical part analyzes the situation, presents the advantages and risks of business of cyberspace. The goal of the questionnaire survey is to find out what are the pitfalls of entrepreneurs in the virtuál environment and how they solve them. The contribution of the bachelor thesis is the proposal of possibillities for safe business in cyberspace.

Key words

Business, cyberspace, cyber security, threats of the virtuál world.

Prohlašuji, že předložená bakalářská práce je původní a zpracoval/a jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem v práci neporušil/a autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, v platném znění, dále též „**AZ**“).

Souhlasím s umístěním bakalářské práce v knihovně VŠPJ a s jejím užitím k výuce nebo k vlastní vnitřní potřebě VŠPJ.

Byl/a jsem seznámen/a s tím, že na mou mé bakalářskou práci se plně vztahuje **AZ**, zejména § 60 (školní dílo).

Beru na vědomí, že VŠPJ má právo na uzavření licenční smlouvy o užití mé bakalářské práce a prohlašuji, že **s o u h l a s í m** s případným užitím mé bakalářské práce (prodej, zapůjčení apod.).

Jsem si vědom/a toho, že užít své bakalářské práce či poskytnout licenci k jejímu využití mohu jen se souhlasem VŠPJ, která má právo ode mne požadovat přiměřený příspěvek na úhradu nákladů, vynaložených vysokou školou na vytvoření díla (až do jejich skutečné výše), z výdělku dosaženého v souvislosti s užitím díla či poskytnutím licence.

V Jihlavě dne: 8. 4. 2019

…….
Podpis studenta/ky

Poděkování

Ráda bych poděkovala vedoucí bakalářské práce Ing. Dagmar Frendlovské, Ph.D., za její připomínky, cenné rady a podporu při zpracování této práce. Dále chci poděkovat všem respondentům, kteří se účastnili dotazníkového šetření. V neposlední řadě bych chtěla poděkovat své rodině a přátelům za pomoc a podporu, které se mi od nich dostávalo v průběhu mého studia.

Obsah

Seznam použitých zkratek

FO fyzická osoba

PO právnická osoba

s.r.o. společnost s ručením omezeným

a.s. akciová společnost

v.o.s. veřejná obchodní společnost

k.s. komanditní společnost

CRM customer relationship management (v překladu management zaměřený na vztahy se zákazníky)

CR cestovní ruch

ZBK zákon o kybernetické bezpečnosti

TK trojský kůň

UZ ubytovací zařízení

ICT informační komunikační technologie

Úvod

Dnešní doba je nazývána dobou elektronickou. Na internetu lze nalézt téměř cokoli. Zároveň si přes internet můžete pořídit takřka jakékoli služby či produkty. Internet neboli kyberprostor se stále rozvíjí a s jeho rozvojem dochází i k významnému rozvoji podnikání v něm. S rozvojem kyberprostoru přichází ale i rizika v podobě narušení bezpečnosti.

Bakalářská práce se zabývá podnikáním v kyberprostoru a nástrahami, které sužují podnikatele a v konečném důsledku i finální spotřebitele. Kyberprostor umožňuje podnikatelům a firmám lepší a rozsáhlejší propagaci. Zároveň jde o snadný způsob nákupu produktů a služeb. Součástí nákupu přes internet je zadávání citlivých údajů. Ty mohou být snadno zneužity, pokud není webová stránka, z níž zákazník nakupuje, dostatečně zabezpečena. Mohou také uniknout citlivé informace o firmě, které mohou být pro firmu likvidační, a to v případě, že se kybernetický zločinec naboural do systému firmy. Z tohoto důvodu byl 1. 1. 2015 vyhlášen Zákon o kybernetické bezpečnosti č. 181/2014 Sb. Firma je také chráněna Nařízením vlády č. 315/2014 Sb., ze dne 8. 12. 2014. Tato opatření však mnohdy nestačí, a proto je nutné, aby si podnikatelé webové stránky zabezpečili a tím eliminovali útoky zločinců v kyberprostoru.

V teoretické části se budu věnovat terminologii a vysvětlení základních pojmů, jako jsou kyberprostor, kybernetická bezpečnost, podnikání v kyberprostoru a hrozby ve virtuálním světě. Proto, že jsem studentkou cestovního ruchu, je práce zaměřena na druhy podnikání v kyberprostoru v cestovním ruchu. Nejprve vymezím termín cestovní ruch a poté uvedu tabulku, v níž jsou znázorněny druhy podnikání v oblasti cestovního ruchu ve virtuálním světě.

Praktická část obsahuje tři různé dotazníky pro lepší pochopení tématu ze všech úhlů pohledu a jejich vyhodnocení. Nejprve jsou dotazovanými podnikatelé a cílem dotazníku je zjistit, jakým způsobem zabezpečují své webové stránky. Druhý dotazník je určený pro poskytovatele webhostingu. Cílem je zjistit nejčastější rizika, hrozby a nástrahy, které sužují podnikatele ve virtuálním světě. Dále také ochranné prvky, za jejichž pomoci jsou tyto hrozby eliminovány. Poslední dotazník je zaměřený na uživatele/nákupčí na webových stránkách a bude doplňujícím údajem o nákupním chování zákazníků.

Otázky jsou směrovány na zjištění informací o tom, zda nakupují online, jestli mají při nakupování online obavy a popřípadě jaké. Dotazníky jsou vyhotoveny jak v ústní, tak i v elektronické podobě. Na závěr budou zjištěné výsledky doplněny o porovnání web-hostingových firem s návrhem na ideální zabezpečení pro internetové podnikání v cestovním ruchu.

Motivace

Téma „Kybernetická bezpečnost pro podnikání v kyberprostoru v oblasti cestovního ruchu“ jsem si vybrala z toho důvodu, že bych v budoucnu ráda měla vlastní firmu podnikající v oblasti cestovního ruchu. V dnešní době je kyberprostor součástí takřka každého typu podnikání. Zvláště pak podnikání v cestovním ruchu je závislé na online prostředí. Jedná se o velmi účinný marketingový nástroj, s jehož pomocí je například propagace opravdu snadná, rychlá a účinná. I na tento fakt budu muset v budoucnosti brát zřetel, a proto beru toto téma jako jedinečnou příležitost dozvědět se více o samotném virtuálním světě. Jsem přesvědčena, že si díky této práci rozšířím své znalosti o obraně před potenciálními hrozbami v internetovém prostředí. Zároveň si díky těmto informacím připravím takzvanou „rodnou půdu“ pro vytvoření svých vlastních stránek, které budou mít za úkol v budoucnu zaujmout potenciální zákazníky a já jim budu schopna lépe nabídnout své produkty a služby.

Od práce očekávám nabytí nových informací o hrozbách ve virtuálním světě. O způsobu, jakým podnikatelé zajišťují zabezpečení svých webových stránek. Zajímá mne, zda své stránky svěřují externí firmě, anebo mají v rámci své firmy vlastní tým, který zabezpečuje bezproblémový chod internetových stránek. Věřím, že se mi podaří odhalit metody, jakými se podnikatelé chrání před kybernetickými zločinci.

Cíl práce

Cílem práce je představit problematiku „Kybernetické bezpečnosti pro podnikání v kyberprostoru v CR“ a zjistit, jak podnikatelé řeší zabezpečení svých webových stránek, jak se chrání před možným napadením zločinců ve virtuálním světě. Bakalářská práce obsahuje část teoretickou a část praktickou. V teoretické části jsou vysvětleny pojmy jako například kyberprostor, jeho zabezpečení, cestovní ruch, podnikání v kyberprostoru a s tím spojeny i formy podnikání pohybující se ve virtuálním světě v oblasti cestovního ruchu. Praktická část je zaměřena na uvedenou problematiku z praktického hlediska a obsahuje tři výzkumné části. V první části jsou respondenti podnikatelé v cestovním ruchu, kteří své služby či produkty nabízejí prostřednictvím internetových stránek. V druhé části jsou dotazovanými externí firmy zajišťující webhosting. Poslední částí výzkumu je dotazník určený pro zákazníky a uživatele kyberprostoru jako místa, kde mohou nakupovat služby CR. Dotazník pro zákazníky je součástí práce kvůli pochopení tématu ze všech úhlů pohledu. Pomůže nám zjistit, jak jsou zákazníci a jejich chování ovlivňováno hrozbami ve virtuálním světě. Na konci práce bude uvedená tabulka se srovnáním webhostingových firem, které podle vybraných parametrů mohou být pro podnikatele těmi nejvýhodnějšími.

1 Teoretická část

1.1 Podnikání

Interpretace pojmu podnikání není úplně jednoduchá a dá se pojmout z více hledisek.

1) Ekonomické pojetí – podnikání je zapojení ekonomických zdrojů a jiných aktivit tak, aby se zvýšila jejich původní hodnota. Je to dynamický proces vytváření přidané hodnoty. (Veber, Srpová a kolektiv, 2012)

2) Psychologické pojetí – podnikání je činnost motivovaná potřebou něco získat, něčeho dosáhnout, vyzkoušet si něco, něco splnit. Podnikání v tomto pohledu je prostředek k dosažení seberealizace, zbavení se závislosti, postavení se na vlastní nohy apod. (Veber, Srpová a kolektiv, 2012)

3) Sociologické pojetí – podnikání je vytvářením blahobytu pro všechny zainteresované, hledáním cesty k dokonalejšímu využití zdrojů, vytvářením pracovních míst a příležitostí. (Veber, Srpová a kolektiv, 2012)

4) Právnické pojetí – podnikáním se rozumí soustavná činnost prováděná samostatně podnikatelem vlastním jménem a na vlastní odpovědnost za účelem dosažení zisku. (Zákon č. 513/1991 Sb., obchodní zákoník)

Samostatná činnost spočívá v tom, že fyzická či právnická osoba samostatně rozhoduje o tom:

1) jaké statky nebo služby bude poskytovat,

2) jakým způsobem a kde bude tyto produkty vytvářet,

3) s kým bude spolupracovat

4) jakým způsobem bude financovat provoz

5) jakou právní formu pro své podnikání zvolí

6) jak bude vytvářet ceny

I pro pojem podnikatel se nabízí více definic. Dle zákona č. 513/1991 Sb., obchodník práce – Podnikatel je osoba, zapsaná v obchodním rejstříku, podniká na základě

živnostenského oprávnění nebo na základě jiného než živnostenského oprávnění podle zvláštních předpisů.

Další definicí podnikatele je: Podnikatel je osoba realizující podnikatelské aktivity s rizikem rozšíření nebo ztráty vlastního kapitálu. Osoba schopná rozpoznat příležitost, mobilizovat a využívat zdroje a prostředky k dosažení stanovených cílů a ochotná postoupit tomu odpovídající rizika. Iniciátor a nositel podnikání – investuje své prostředky, čas, úsilí a jméno, přebírá odpovědnost, nese riziko s cílem dosáhnout svého finančního a osobního uspokojení. (Veber, Srpová a kolektiv, 2012)

Pokud se fyzická osoba – podnikatel – nechá zapsat do obchodního rejstříku, pak zápisem do obchodního rejstříku se podnikateli – fyzické osobě – určitým způsobem mění práva a povinnosti. Například fyzická osoba, která je zapsaná do obchodního rejstříku, může zřídit odštěpný závod, může ustanovit prokuristu, má ochranu firmy, protože její jméno a příjmení pod nímž podnikala, se stalo obchodní firmou. Nic z tohoto nemůže realizovat nezapsaná fyzická osoba.

Obchodní společnosti jsou právnické osoby, založené za účelem podnikání. Jedná se v podstatě o zvláštní právní formu sdružování osob (fyzických i právnických) ke společnému výkonu podnikání. Tyto společnosti jsou: s.r.o., v.o.s., k.s. (Salachová, 2012)

Kromě toho může být také společnost založena pouze jedinou osobou (fyzickou i právnickou) a to u akciové společnosti (a.s.).

1.1.1 Podnikání v kyberprostoru

Elektronickým podnikáním rozumíme sérii procesů majících jasně srozumitelný účel, zahrnující více než jednu organizaci, realizovaných prostřednictvím výměny informací a řízených směrem k vzájemně odsouhlaseným cílům, které probíhají během daného časového intervalu. (Suchánek, 2012)

Podnikání v kyberprostoru můžeme rozdělit na různé modely elektronického podnikání.

1) E-business = je elektronické podnikání související s rozvojem internetu a telekomunikací. Součástí e-businessu je e-commerce, ale také *CRM systémy* (= Jsou to systémy pro řízení vztahů se zákazníky. Programy umožňující shromažďovat, třídit a zpracovávat údaje o zákaznících.), *intranet* (= Druh webové prezentace, která sdílí informace v rámci firmy např. přehledy novinek, seznam odkazů na soubory atd. Pomáhá zefektivnit vnitrofiremní procesy), *extranet* (= Aplikace, která slouží ke sdílení citlivých informací s uživateli, nejčastěji se spolupracujícími firmami, obchodními zástupci i s koncovými zákazníky. Informace nejsou dostupné volně jako u běžných webových stránek, ale až po autorizaci.) atd.[1]

2) E-commerce = (= e-komerce) je elektronické obchodování (internetové obchody). Tento pojem je používán k označení obchodních transakcí realizovaných za pomoci internetu. Je součástí elektronického podnikání (e-businessu). E-komerci můžeme rozlišit podle cílové skupiny a to na: B2B e-komerci (zaměřenou na obchodníky) a B2C e-komerci (zaměřenou na konečné zákazníky). [2]

3) E-shop = elektronický obchod/internetový obchod/online obchod. Jedná se o webovou aplikaci, která slouží ke zprostředkování obchodních transakci online, a to převážně formou B2C.[3]

4) E-government = takto se označuje možnost komunikace s institucemi státní a veřejné správy v elektronické podobě a s tím související procesy. Také tvorba příslušné legislativy a přechod úřadů na elektronickou verzi.[4]

5) E-banking = elektronické bankovnictví

Podnikání v kyberprostoru vyžaduje subjekty, které mezi sebou uzavírají obchody. Dělí se tedy na ty, kteří tvoří poptávku a na ty, kteří tvoří nabídku. V následující tabulce jsou uvedeny jednotlivé modely podnikání v kyberprostoru.

1 http://www.adaptic.cz/znalosti/slovnicek/e-business/
2 http://www.adaptic.cz/znalosti/slovnicek/e-commerce/
3 http://www.adaptic.cz/znalosti/slovnicek/e-shop/
4 http://www.adaptic.cz/znalosti/slovnicek/e-government/

Tabulka 1: Modely podnikání v kyberprostoru

Zkratka	Dodavatel a Odběratel	Charakteristika
B2B	Obchodník – obchodník	Obchodní vztahy a vzájemná komunikace mezi dvěma společnostmi. B2B vztahy většinou fungují na principu elektronické výměny dat, jako například objednávky či faktury. Nejsložitější B2B systémy potom fungují jako komunikační a distribuční komunikační a distribuční sítě, sloužící k regulaci již navázaných obchodních vztahů.
B2C	Obchodník – zákazník	Zahrnuje přímý prodej koncovým zákazníkům. Základem služeb B2C je snaha informovat o produktech. Webová stránka pak plní funkci letáku či elektronického katalogu. Vyšší úroveň B2C služeb pak přidává interaktivní formuláře například pro možnost zpětné vazby.
B2A	Obchodník – veřejná instituce	Obchodní a komunikační vztahy obchodníků s veřejnými institucemi. Jedná se o vztahy na nižší úrovni státní správy (např. místní samospráva). Do této kategorie lze zařadit také komunikaci obchodníků s finančními institucemi.
B2G	Obchodník – veřejná instituce	Obchodní vztahy a komunikace s úřady a orgány státní správy. Jedná se o nabídku produktů institucím státní správy a také veškerá komunikace s těmito zařízeními. Typickým

		příkladem může být například možnost podávat daňová přiznání s využitím elektronického podpisu.
B2R	Podnik – obchodní zástupce	Obchodní vztahy a komunikace mezi obchodníkem a jeho obchodními zástupci. V B2R jde především o vzájemnou výměnu strukturovaných dat. Používají se různé druhy extranetu (webová aplikace sloužící ke sdílení citlivých informací nejčastěji s obchodními zástupci, spolupracujícími firmami, s koncovými zákazníky).

(Zdroj: Janková, Frendlovská 2013)

1.2 Kyberprostor

Kyberprostor (z anglického *Cyberspace*) je označení pro virtuální realitu. Je to realita, která je nedílnou součástí počítačového světa. Slovem kyberprostore se dá zjednodušeně označit veškerý internet jako takový.
David Hakken charakterizuje kyberprostor jako sociální arénu, do níž vstupují uživatelé používající pokročilé informační technologie ke vzájemné komunikaci. Přirovnává kyberprostor k životnímu stylu, ke kultuře vytvořené pomocí informačních technologií. Tato kultura je pak tvořena množstvím technik, vztahů a artefaktů z oblastí informačních a komunikačních technologií.

Dle zákona o elektronických komunikacích se kybernetickým prostorem rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.

Kybernetický prostor nemá hmotnou podstatu, je imaginární. Jeho vznik a další existence je však závislá na světě reálném.

1.3 Kybernetická bezpečnost

Je třeba, aby každý provozovatel informačního a komunikačního systému, který by mohl mít skutečný či potenciální význam pro fungování státu, regionu, města nebo významné organizace, a to bez ohledu, zda na něj dopadají či nedopadají povinnosti podle ZBK, uskutečnil následující kroky:

1) Provést analýzu rizik,
2) Zpracovat koncepci minimalizace existujících rizik,
3) Navrhnout a realizovat proaktivní opatření za účelem snížení zjištěných rizik,
4) Monitorovat, vyhodnocovat a operativně modifikovat tato opatření. (Smejkal, 2013)

1.4 Hrozby kyberprostoru

Virtuální svět neboli kyberprostor má jednu velmi důležitou vlastnost. Je jí anonymita. V tomto prostoru se může pohybovat každý, a pokud nemá zájem o to, aby o něm další uživatelé věděli, je to velmi snadno proveditelné. Například prostřednictvím remailerů mohou uživatelé zajistit to, že se příjemce emailové zprávy nedozví, kdo je odesílatelem. Má to však své světlé i stinné stránky. Na jednu stranu jde o jakési pohodlí uživatelů. Na straně druhé dává virtuální svět příležitost lidem (hackerům, crackerům, zločincům atd.), kteří chtějí škodit ostatním. Jedná se potom o kyberkriminalitu. O kyberkriminalitě mluvíme tehdy, kdy se trestné činy odehrávají v rámci celého kyberprostoru.[5]

Nejčastěji se jedná o útoky na bankovní a e-mailové účty, kdy se útočník snaží zjistit heslo a ukrást osobní data. Pomocí emailových zpráv může rozesílat nevyžádanou poštu tedy newslettery. Motivy pro konání těchto činů mohou být různé (např. osobní msta z důvodu vyhazovu z práce, rozchodu, antipatie vůči druhé osobě apod.). V každém případě se jedná o činnost nemorální a nelegální. Pokud tuto činnost páchá pouze jedna osoba může se jednat o kybergrooming (=specifický případ kyberkriminality, kdy se pachatel tváří jako důvěryhodná osoba a například se snaží přimět mladistvé ke schůzce

[5] https://www.sprava-site.eu/kyberprostor/

za účelem jejich fyzického zneužití). Kybergrooming často hraničí s kyberstalkingem a může přerůst v kyberšikanu.[6]

V této bakalářské práci se zaměříme ale především na druh kyberkriminality, kdy je cílem pachatelů prolomit kódy a dostat se neoprávněně do systému, aby zde odcizovali, pozměňovali, nebo dokonce ničili data. Tuto činnost provádí crackeři. S oblibou také zavádějí do systémů viry a získávají čísla kreditních karet. V případě, že se na kyberkriminalitě podílí celá organizace lidí z celého světa, může jít o cílený kyberterorismus (tento typ kyberkriminality je ale využíván především zločinci, kteří mají v úmyslu uškodit velké skupině lidí. Např. státu, vládě, nadnárodním organizacím atd.).[7]

Pro dosažení svých cílů používají crackeři specifické metody.

1) Phishing = (v překladu „rybaření“) útočník rozesílá mail, v něm se vydává za banku a požaduje buď sdělení určitých údajů, nebo provedení nějaké operace (např. kliknutí na přiložený odkaz). Cílem podvodných emailů je získání přihlašovacích údajů k internetovému bankovnictví, PINů platebních karet nebo dalších bezpečnostních údajů k různým finančním službám nebo serverům pro obchodování na internetu (PayPal, eBay, Amazon, Paysec apod.). (Smejkal, 2015)

2) Pharming = (v překladu „farmaření“) útočník využívá speciální počítačové programy, které jsou v podstatě viry nebo se také označují jako „malware“. Jsou to škodlivé programy a uživatele při přihlášení do internetového bankovnictví přesměrují na stránky, jež vypadají jako originální stránky, ale ve skutečnosti jsou pouze jejich napodobeninou. Zde požádají klienta o zadání všech přihlašovacích informací. (Smejkal, 2015)

3) Trojský kůň = jeden z nejrozšířenějších typů malwaru. Jedná se o skrytou část programu nebo aplikace, která má provozovat svou sabotující činnost. Primární úkol TK je vytvoření tzv. back door (=druh kódu, díky kterému cracker může

[6] https://www.sprava-site.eu/kyberkriminalita/
[7] https://www.sprava-site.eu/kyberkriminalita/

snadno převzít kontrolu nad infikovaným počítačem, aniž by si toho majitel všimnul). [8]

4) Hoax = falešná zpráva varující před neexistujícím nebezpečím. Jeho typickým znakem je, že zpráva obsahuje výzvu, aby byl šířen dále mezi další uživatele. Hoax je specifická forma spamu a mohou také spadat pod malware, tedy škodlivé programy.[9]

5) Sniffing = technika umožňující odposlouchávání počítačů v lokální síti, která se používá např. při diagnostice sítě. Sniffing nahrazuje činnost spywaru (špionáž dat) či keyloggeru (zjištění hesel).[10]

6) Brute force = (neboli útok hrubou silou) je druh útoku, kdy cracker pomocí tohoto programu zjistí uživatele a jeho hesla. Nepotřebuje k tomu žádné šifrovací klíče. Funguje na principu postupného vytváření všech možných kombinací. V prolamování hesel může být kombinován s dalšími metodami – např. slovníkový útok (= cracker předem připraví databázi slov, ze kterých zkouší použít různé varianty na prolomení ochrany uživatelského účtu či systému).[11]

V rámci kyberprostoru také existuje místo, které se nazývá Darknet. Jedná se o temnou stránku internetu, privátní síť, kam se dostanou pouze ti, kteří znají jiného uživatele přímo této sítě. V této části kyberprostoru se neřeší zákony ani právní ani morální a využívá se zde spojení peer to peer neboli rovný s rovným (P2P). (Smejkal, 2015), [12]

1.5 Cestovní ruch

Cestovní ruch je významným sektorem národního hospodářství. V průběhu 20. století jeho význam vzrostl a stal se běžnou součásti života obyvatel vyspělých států. (Linderová, 2013)

Vznik a rozvoj novodobého cestovního ruchu předpokládá:

1) Možnost svobodného pohybu lidí,

8 https://www.sprava-site.eu/trojsky-kun/
9 https://www.sprava-site.eu/hoax/
10 https://www.sprava-site.eu/sniffing/
11 https://www.sprava-site.eu/brute-force/
12 https://cemolid.blogspot.com/2015/04/darknet-internetove-podsveti.html

2) Existence primární nabídky, která je základem tvorby produktu jako předmětu spotřeby v CR,
3) Takový stupeň technického, ekonomického a sociálního rozvoje, který má za následek postupné zkracování fondu pracovní doby a prodlužování fondu volného času,
4) Takový stupeň uspokojená základních životních potřeb, kdy vzniká možnost uspokojovat i méně nezbytné potřeby, kam řadíme i CR a výstavbu potřebných dopravních, ubytovacích, pohostinných, sportovně-rekreačních a dalších zařízení pro CR. (Gúčik, 2001)

Podle W. Hunzikera a K. Krapfa je cestovní ruchu: „Soubor jevů a vztahů, vyplývajících z pohybu osob na cizím místě, pokud cílem pobytu není trvalé usazení nebo výkon výdělečné činnosti.“ (Gúčik, 2010)

1.6 Formy podnikání v kyberprostoru v oblasti cestovního ruchu

Firem, které působí na internetu a podnikají v oblasti CR je velká spousta. Pro cestovní ruch je nepostradatelná doprava. Je velmi důležité, aby v zemi existovala flexibilní, na sebe navazující dopravní síť v rámci celého území. Česká republika má provázanou autobusovou a železniční dopravu, také disponuje leteckou dopravou na středně dlouhé vzdálenosti. Nesmíme opomenout lodní dopravu, která je ale spíše rekreační.

Následuje ubytování, bez kterého by cestovní ruch jen velmi těžko mohl fungovat. Zaměříme se na portál nabízející ubytování a pak také příklady ubytování ve vybraném městě.

Další částí jsou cestovní kanceláře a agentury. Dále pojišťovny zřizující cestovní pojištění a v neposlední řadě i organizace, které se zabývají cestovním ruchem.

Všechny uvedené společnosti podnikají v kyberprostoru.

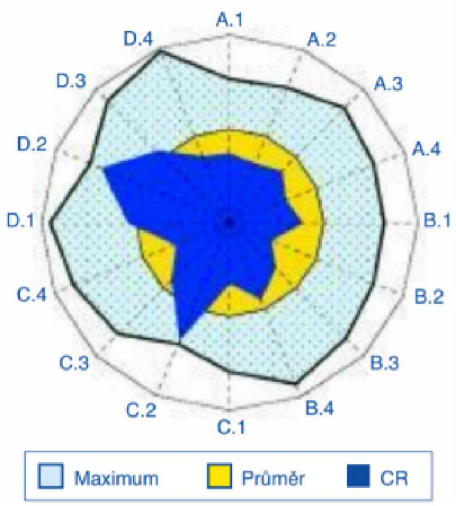
V následující tabulce jsou znázorněny formy podnikání, které disponují webovými stránkami. Kromě vlakové a letecké dopravy jsou všechny formy podnikání vyhledávány v kraji Hlavního města Prahy. Vlaková a letecká doprava je uvedena v rámci celého území ČR.

Tabulka 2: Formy podnikání v oblasti CR

Forma podnikání	Druh společnosti	Místo	Počet společností
Doprava	Autobusová	ČR	Více než 6
	Vlaková	ČR	3
	Letecká	ČR	2
	Lodní – říční	Vltava	6
CK	Kamenné i internetové obchody	Praha	Více než 36
CA	Kamenné i internetové obchody	Praha	Více než 8
Ubytování	Hotel/hostel	Praha	Více než 450

Zdroj: vlastní zpracování

Ministerstvo pro místní rozvoj zveřejnilo v roce 2008 graf, který znázorňuje využití ICT ve firmách v CK. Na grafu č. 1 můžeme vidět bod D2, kde jsou hodnoty pro CR na linii maxima, viz popisek (obrázek č. 1). Oblast D zastupuje marketing a prodej a bod D2 přijímání objednávek online.



Graf 1: Využití ICT ve firmách v CR

Zdroj: Mmr.cz, 2008

Indikátor (% firem)

A. ICT sítě
A.1 Internetové připojení
A.2 LAN
A.3 W-LAN
A.4 Vzdálené připojení do firemní sítě

B. Integrace firemních procesů
B.1 Intranet
B.2 ERP Systémy
B.3 Online sledování výrobního času
B.4 E-fakturace

C. Dodavatelské systémy
C.1 Online objednávky
C.2 Systémy pro výběr nejlepšího dodavatele
C.3 Napojení na systémy dodavatele
C.4 Online řízení zásob

D. Marketing a prodej
D.1 Použití CRM
D.2 Přijímání objednávek online
D.3 Systémy pro marketing a prodej
D.4 Napojení na systémy zákazníka

1. Obrázek: Popisek ke grafu č. 1

Zdroj: Mmr.cz, 2008

2 Praktická část

Praktická část bakalářské práce je zaměřena na fungování nabídek v cestovním ruchu na internetu. K přiblížení a lepšímu pochopení tématu jsem použila dotazníkové šetření, ve kterém budu zjišťovat pohled na kybernetickou bezpečnost pro podnikání v něm z různých úhlů, k čemuž mi pomohou tři různá výzkumná šetření. Proto bude praktická část rozdělena na tři výzkumné části.

Nejdříve jsou dotazovanými společnosti. Jedná se o krátký dotazník, ve kterém se snažím zjistit, zda si podnikatelé zabezpečují své webové stránky sami nebo tuto otázku řeší prostřednictvím externí firmy. Tento první výzkum je provedený v ústní i písemné formě – na základě telefonické komunikace a následně i v emailové podobě pro obtížnost zjištění telefonického kontaktu na kompetentní osobu. Bylo osloveno 30 firem a tato část výzkumu je zcela anonymní.

Druhá část výzkumu je provedena formou rozhovoru, který je zacílen na společnost poskytující webhosting (společnost nabízející pronájem „vlastního prostoru na internetu“, správu webových stránek ve smyslu zabezpečení a dohledem nad webem). Cílem tohoto rozhovoru je zjistit nejčastější hrozby, které ohrožují podnikatele ve virtuálním světě a kdo je obvykle provádí. Jakým způsobem se tyto hrozby řeší a jak se jim dá předejít. Rozhovor je proveden především v telefonické podobě, ale i na základě osobního setkání a bylo osloveno 7 společností.

Poslední dotazník je určen pro cílové zákazníky. Tento dotazník jsme vytvořila z toho důvodu, abych získala data pro úplný náhled na danou problematiku. Dotazník byl vyhotoven v písemné podobě a zahrnuje 14 otázek. Zjišťovala jsem v nich informace o nákupním chování zákazníků s orientací na nákup služeb/produktů cestovního ruchu a formy placení, které upřednostňují. Hlavním cílem dotazníku však bylo získání informací týkajících se povědomí o hrozbách ve virtuálním světě a jejich dopad na nákupní chování nákupčích. Pro tento dotazník bylo osloveno 160 respondentů.

Zjištěná data jsem vyhodnotila a na závěr vyhotovila tabulku se srovnáním 5 firem poskytujících webhosting na českém trhu, které by dle parametrů měly být těmi nejvýhodnějšími pro podnikatele.

2.1 Výzkumné metody sběru dat

Jako metodu výzkumného šetření pro sběr dat jsem použila kvantitativní i kvalitativní výzkum. Kvantitativní výzkum jsem provedla písemným dotazováním a kvalitativní rozhovorem. První části výzkumu se účastnilo 30 firem/společností podnikajících v oblasti cestovního ruchu v kyberprostoru a byla použita metoda dotazování. Druhá část byla provedena formou rozhovoru a této části se účastnilo 7 firem poskytujících webhosting. Poslední částí je online dotazníkové šetření, kterého se zúčastnilo 160 respondentů. Tito respondenti byli vybráni tak, aby se jednalo o zákazníky, kteří jsou uživateli kyberprostoru.

2.2 Techniky dotazování

Při sběru dat byla použita ústní (telefonicky i osobně), písemná (tištěná) a online technika.

V první výzkumné části byli respondenti formou dotazováni v ústní (telefonickou) a online podobě. Jedná se o dvě krátké otázky, které byly kladeny telefonicky a následně i formou emailu. Email byl vytvořen v jazyce českém i anglickém v závislosti na národnosti osoby, která odpovídala za mnou vybranou firmu. V českém jazyce odpovědělo sedm firem a v anglickém jedna. Tato část výzkumu byla anonymní. V práci nebudou sděleny názvy společností a firem podílejících se na výzkumu.

Druhá výzkumná část byla provedena pouze v ústní (telefonické i osobní) formě v podobě rozhovoru pomocí návodu. Jedná se o polostrukturovaný rozhovor, který stojí na pomezí strukturovaného a nestrukturovaného rozhovoru. (Linderová, Scholz, Munduch, 2016). Pouze v druhé výzkumné části budou uvedeny názvy firem, které byly součástí výzkumu.

Pro poslední výzkumnou část byl použit elektronický dotazník, který jsem vytvořila pomocí aplikace Formuláře Google. I tato část výzkumu byla anonymní. V práci nebudou sděleny žádné citlivé údaje o osobách podílejících se na výzkumu.

Emaily k první výzkumné části naleznete v příloze A Email. Rozhovor použitý v části dvě naleznete v příloze B Rozhovor a celý online dotazník naleznete v příloze C Dotazník.

2.3 Výzkumná část 1

V první výzkumné části jsou dotazovanými firmy/společnosti, které podnikají v kyberprostoru. Metodou sběru dat je dotazování formou jak telefonickou, tak i emailovou.

Nejprve jsem všechny respondenty kontaktovala telefonicky, ale pro obtížnost získání kontaktu na kompetentní osobu jsem přešla k dotazování pomocí emailové zprávy.

2.3.1 Charakteristika respondentů

Oslovených firem bylo 30 a byly to největší a nejvýznamnější firmy podnikající v oblasti cestovního ruchu ve virtuálním světě. Tyto firmy jsem si rozdělila na kategorie dopravci, hoteliéři, cestovní kanceláře a agentury, pojišťovny a organizace v cestovním ruchu.

Kategorie doprava byla rozdělena na její druhy a to: autobusovou, železniční, leteckou a lodní. Mezi dopravci byli například společnosti, které na trhu působí už 100 let. Někteří z nich jsou „nováčky“ a provozují dopravu v České republice od roku 1996 a jiný se pyšní přepravou až 5000 pasažérů za den. V kategorii hoteliérů byli respondenty portály nabízející ubytování, dále různé kategorie ubytovacích kapacit – od hotelů, přes hostely po penziony a apartmány. Mezi CK a CA se nacházejí firmy poskytující českým zákazníkům své služby téměř 100 let. Také společnost, která za rok 2017 odbavila 315 tisíc zákazníků nebo například firma, která má ve své nabídce 28 letovisek, 582 možností ubytování a až 366 975 termínů, ze kterých si jejich klienti mohou vybrat to pravé pro ně.

2.3.2 Použité otázky

Jak již bylo výše zmíněno, nejprve jsem kontaktovala všechny dotázané telefonicky. Šlo mi o kontaktování kompetentní osoby, která bude schopná zodpovědět mé otázky na zabezpečení jejich webových stránek. V drtivé většině jsem se setkala s odkazem na emailovou zprávu, která poté byla přeposlána osobě zodpovědné v této oblasti pro danou firmu/společnost.

Emailová zpráva obsahuje představení autora práce, představení práce a vysvětlení, proč se obracím právě na tu danou společnost/firmu. Následují dvě otevřené otázky, díky kterým jsem získala data o zabezpečení jejich webových stránek. První otázka zněla: *Zajišťujete si vy, jako firma, zabezpečení webových stránek sami v rámci vaší firmy/společnosti?*

Navazovala další otázka, která byla relevantní v případě, že si firma/společnost nezajišťovala zabezpečení sama v rámci té dané firmy/společnosti: *V případě, že ne, máte zajištěné zabezpečení od externí firmy? Pokud ano, o jakou firmu se jedná?* Na základě individuálních odpovědí jsem měla připraveny další doplňující otázky.

2.3.3 Výsledky výzkumné části 1

Z celkového počtu 30 dotázaných firem (100 %) bylo 12 firem (40 %), které nemohly sdělit informace týkající se zabezpečení jejich webových stránek. Tento verdikt jim vydalo podle jejich slov vedení jejich společnosti. Dostávalo se mi odpovědí, že se týká o citlivé informace, a proto nemohou sdělit ani informaci, zda si zabezpečení svých webových stránek zajišťují sami nebo skrze externí firmu. Jejich odpovědi rozumím tak, že i toto je jeden ze způsobů zajištění bezpečnosti proti možné hrozbě. A i přesto, že byli informováni o anonymitě tohoto výzkumu mi požadovanou odpověď neposkytli.

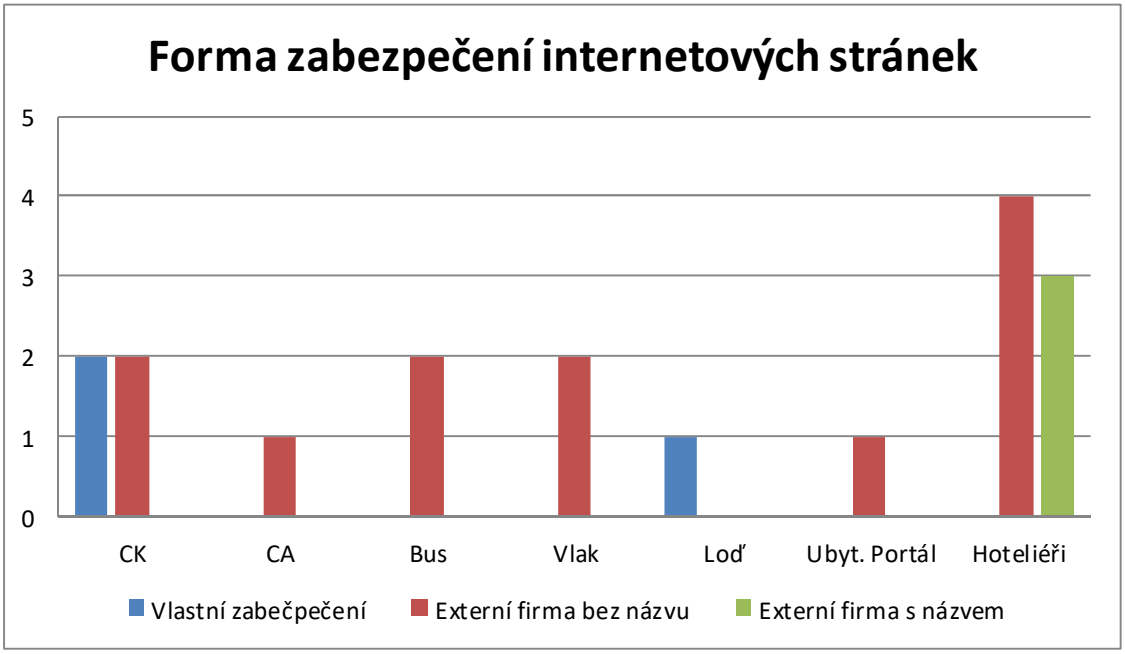
Mezi 12 firmami/společnostmi, které mi nemohly nebo nechtěli tuto informaci sdělit byly převážně největší společnosti poskytující dopravu a pojištění. Tuto informaci si také chránily cestovní kanceláře a agentury.

Mezi zbylých 18 firem (60 %) se zařadily 2 CK (6,7 %), u kterých byla zaškrtnuta odpověď, že si zabezpečení webových stránek zajišťují sami v rámci jejich firmy. Dále mi však nechtěli poskytnout informace o tom, jak se chrání před nástrahami kyberprostoru ani další informace týkající se rizik podnikání v kyberprostoru. Stejný výsledek jsem zaznamenala u 1 lodní společnosti (3,3 %).

Dalších společností, které byly ochotny odpovědět na otázku, a to přímo telefonicky, bylo osm: 2 CK (6,7 %), 1 CA (3,3 %), 1 ubytovací portál (3,3 %), 2 společnosti poskytující autobusovou dopravu (6,7 %) a 2 společnosti poskytující vlakovou dopravu (6,7 %). Všechny tyto společnosti využívají externí firmu pro zabezpečení jejich webových stránek. Kvůli bezpečnosti však žádný z nich nebyl ochotni sdělit název firmy, která se o zabezpečení stará.

Hoteliéři byli všeobecně nejvíce ochotni poskytnout informaci týkající se formy zabezpečení jejich internetových stránek. Celkem 7 společností (23,3 %) zodpovědělo tuto otázku a ve všech případech vypověděli, že mají externí firmu, která se stará o zabezpečení jejich stránek. Čtyři společnosti nemohly poskytnout informaci o firmě, která jim zabezpečuje stránky. Zbylí tři hoteliéři byli ochotni sdělit i název externí firmy zabezpečující internetové stránky dané společnosti.

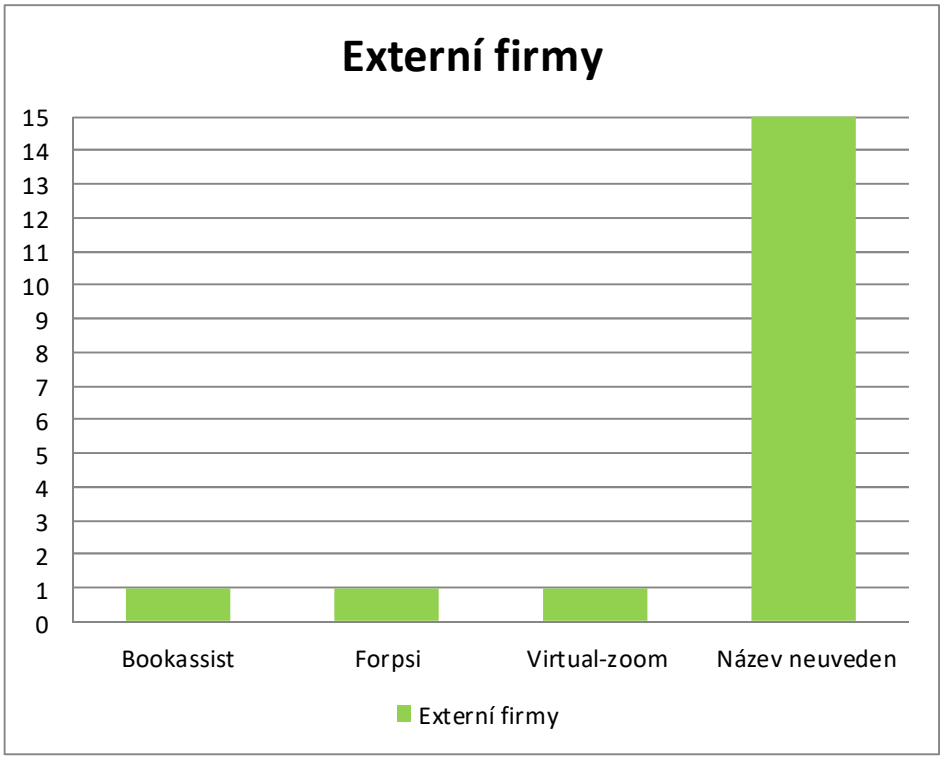
Z mého úhlu pohledu jsou hoteliéři ochotnější poskytnout výše uvedené informace, protože zřejmě mají méně negativní zkušenosti s případným ohrožením jejich webových stránek. Také mluvili převážně o programech zprostředkující ubytování. Lze se domnívat, že takové programy mají již své tovární zabezpečení. Velké firmy byly nejméně ochotny zodpovědět výše uvedené otázky, a to dle mého názoru především proto, že je u nich v sázce více ohrožení než u menších firem. Disponují větším objemem citlivých dat.



Graf 2: Výzkumná část 1 – Forma zabezpečení internetových stránek

(Zdroj: vlastní zpracování)

Jedno nejmenované ubytovací zařízení využívá služeb firmy Bookassist. Jeden hotel je uživatelem webhostingové společnosti Virtual-zoom. Poslední hoteliér ochotný poskytnout název firmy zabezpečující jejich stránky sdělil, že webhostingová společnost zabezpečující chod jejich internetových stránek je společnost Forpsi.



Graf 3: Výzkumná část 1 – Využívané externí firmy

(Zdroj: vlastní zpracování)

Nejprve bych ráda uvedla rizika firem, které se pohybují v kyberprostoru. Firmy, které mají webové stránky jsou ohroženy kybernetickými zločinci, a to ve dvou hlavních bodech. To, co mohou útočníci zneužít jsou: zaprvé data o firmě a zadruhé může dojít k úniku osobních dat zákazníků. Oba tyto případy by mohly pro firmu znamenat konec. V prvním případě, pokud se zločinec naboural do systému, může firmě do systému nainstalovat chybu. Může také ukrást citlivá data o firmě, která v rukou konkurence mohou být pro podnik likvidační. V druhém případě, pokud zcizí osobní údaje o zákaznících bude zničena důvěryhodnost firmy v očích zákazníků, což povede taktéž k likvidaci firmy. Pokud se zločinec naboural do databáze kontaktů, může pak rozesílat newslettery (nevyžádanou poštu) a ta bude obtěžovat klienty. I v tomto případě bude poškozeno jméno firmy.

Z výzkumu jsem však zjistila několik faktů. Zaprvé jsem zjistila, že se většina firem chrání už jen tím, že nikomu cizímu neposkytují žádné informace o chodu firmy, o jejím zabezpečení. Zároveň je velmi obtížné spojit se telefonicky nebo se osobně setkat s člověkem, který řeší zabezpečení té dané společnosti/firmy. I toto je jedním z prvků zabezpečení firmy. Ve většině případů, jak jsem již zmiňovala, jsem byla odkázána na emailovou adresu, kam jsem mohla zaslat své dotazy. Také jsem zjistila, že spíše velké firmy/společnosti nejsou ochotny nebo nemohou sdělit informace týkající se zabezpečení jejich webových stránek. Myslím si, že je to ochrana nejen před zločinci ve virtuálním světě, ale také před konkurencí. Ta by mohla být pro firmu likvidační ve chvíli, kdy by se dostala k citlivým informacím firmy, jak jsem již zmiňovala tuto situaci výše. Z výzkumu jsem se také dozvěděla, že mezi firmami, které mi byly ochotny sdělit informace o zabezpečení jejich webových stránek jsou pouze 3 z 18 firem, které mají na zabezpečení svých webových stránek vlastní lidi. Zbylých 15 firem řeší tuto otázku přes externí firmy poskytující webhosting. Z těchto 15 mi byli ochotni sdělit název externí firmy pouze 3 z nich. Jednalo se pouze o společnosti poskytující ubytování. Firma Bookassist je webhostingovou firmou spravující pouze hotelové webové stránky a stránky ubytovacích zařízení. Na druhou stranu webhostingová firma Forpsi se stará o zabezpečení nejen hotelových stránek, ale i jinak zaměřených internetových stránek. Zoom-virtual je stejně jako Bookassist zaměřený pouze na hotelový webdevelopment. Poskytují správu a editaci webu, rezervační systém pro online nabídku a prodej ubytovacích kapacit.

Podařilo se mi zjistit informace pouze o webhostingových firmách, které jsou využívány hoteliéry nebo podnikateli v oblasti ubytování. Proto jsem se rozhodla, že pro druhý výzkum využiji externí firmy poskytující webhosting nejen hotelům či ubytovacím zařízením, ale i ostatním firmám na virtuálním trhu.

2.4 Výzkumná část 2

Druhou výzkumnou částí je rozhovor se společnostmi, které poskytují a nabízejí webhosting. Jako metoda je použit rozhovor s pomocí návodu. Jde o rozhovor, který stojí na pomezí strukturovaného a nestrukturovaného rozhovoru. K rozhovoru jsem měla připraveny 4 otázky, které jsem pokládala respondentům. Jejich pořadí jsem

měnila podle potřeby v závislosti na aktuálním průběhu rozhovoru. Právě z toho důvodu jsem využila tento typ rozhovoru.

Rozhovor jsem provedla v ústní formě, a to jak v telefonické, tak i při osobním setkání.

2.4.1 Charakteristika respondentů

Výběr respondentů pro výzkum číslo 2 jsem provedla na základě srovnání firem nabízejících webhosting. Vybrala jsem šest firem, které dle parametrů týkajících se ceny, velikosti nabízeného prostoru a podpory byly vyhodnoceny jako nejlepší a nejvyužívanější na českém trhu. Připojila jsem k dotázaným také firmu, která poskytuje tyto služby pouze ubytovacím zařízením.

2.4.2 Použité druhy otázek

Rozhovor obsahuje 4 základní otázky, které byly operativně doplňovány o další dotazy v souvislosti s plynoucím rozhovorem. Díky těmto otázkám zjistíme, jak postupovat v případě tvorby webových stránek s návazností na jejich zabezpečení. První otázka se týkala hrozeb. Ptala jsem se poskytovatelů webhostingu: *Jaké jsou nejčastější hrozby vyskytující se v kyberprostoru, které sužují majitele webových stránek?* Další otázka navazovala na předchozí a týkala se řešení problémů, které mohou nastat. *Jakým způsobem řešíte napadení v kyberprostoru?* Otázka č. 3 zněla: *Dokážete říci, které firmy v oblasti cestovního ruchu (doprava, ubytování, pojišťovny, CK, CA, organizace v CR) jsou nejčastěji těmi napadenými? Dá se jasně říct, který okruh firem v CR je nejnáchylnější na kybernetická napadení?* Poslední základní otázkou je: *Je vůbec možné se vyvarovat případnému kybernetickému napadení? Popřípadě jak?*

2.4.3 Výsledky výzkumné části 2

Jak již bylo zmíněno, celkový počet webhostingových firem, které se podílelo na druhé výzkumné části je 7 (100 %). Tato výzkumná část jako jediná není anonymní.

Dotázané firmy byly:

- **ONEbit**, který byl dle srovnání nejlepších webhostingů pro rok 2018 vyhlášen jako nejlepší firmou poskytující webhosting.
- Druhým nejlepším poskytovatelem byl **Český hosting,** a i tuto společnost jsem kontaktovala.
- Další firmou, která se podílela na druhé části výzkumu je **Bookassist** a je zařazena ve výzkumu, protože zastupuje firmy spravující webové stránky hoteliérům, kteří neodmyslitelně patří do cestovního ruchu.
- Společnost **Savana**, která funguje již 10 let.
- Také firma **Wp neuron**, která se zaměřuje na poskytování služeb spojených s hostováním WordPress (redakčních) stránek. (WP je nejpopulárnější open source redakční systém na světě).
- Dotazník je doplněn o odpovědi od webhostingového poskytovatele **Forpsi**.
- Poslední tázanou společností je **eBola.cz** fungující od roku 1999.

Také jsem na této části spolupracovala s externím poradcem, který se zabývá správou webových stránek a poskytl mi mnoho cenných rad.

Firmu ONEbit jsem kontaktovala telefonicky, vysvětlila jsem jim, oč se jedná. Avšak pro nedostatek času mne požádali, abych jim veškeré otázky zaslala emailem. Stejným způsobem jsem obdržela odpovědi i od firmy Forpsi a Bookassist. Firma Český hosting byla stejně, jako předchozí firmy kontaktována telefonicky. Tato firma mi ihned na mé otázky odpověděla stejně jako společnosti Savana, Wp neuron a eBola.cz.

1) Na první otázku, ve které jsem se ptala na nejčastější hrozby a rizika vyskytující se v kyberprostoru mi odpověděli z firmy **ONEbit** takto: *„Nejčastěji bývají webové prezentace napadány skrze známé chyby v systému, pokud se například jedná o redakční systémy (WordPress, Joomla, Drupal). Zde útočníci využívají neaktuální verze samotných redakčních systémů nebo pluginů, které jsou jejich součástí. Z naší pozice není možné přesně určit, kdo útoky provádí, může jít o*

roboty i jednotlivce, kteří se snaží získat citlivé údaje (osobní údaje, čísla platebních karet apod.) nebo do webové prezentace nahrát svůj škodlivý kód.“

Firma **Český hosting**: „*Tato otázka by měla být spíše směrována na programátora, který vytvořil a přímo se stará o tu danou webovou stránku. Většinou se ale jedná o aplikaci, která je provozována a není dostatečně zabezpečená. Zdrojový kód může obsahovat chyby nebo nějaké rozšíření, které může být případně zneužito. Jedná se o nejčastější způsob napadení. Může se jednat o aplikaci, která je zastaralá nebo nevyužívá nějaké novější doplňky. Starší soubory mohou obsahovat chyby, které mohou být útočníkem použity. Jedná se o jedince, kterým se podaří dostat se do systému a poté ho napadnout, nahrát tam soubory (například rozesílat SPAM domény a podobně). Jedná se tedy o aplikace, které nejsou dále udržované.“*

Na tuto otázku odpověděli z firmy **Bookassist** následovně: *„Největší hrozbou je pro nás zneužití citlivých údajů klientů, kteří rezervují na webových stránkách hotelů, jež jsou partnery Bookassistu. Také je pro ně hrozbou zneužití platebních údajů klientů. Na otázku, kdo obvykle provádí tuto nelegální činnost mi nebyli schopni odpovědět s určitostí. Odpověděli pouze, že jsou to zločinci, kteří disponují schopnostmi nabourat se do systému a mají k tomu nějaký záměr.“*

Na společnost **Savana** jsem se obrátila telefonicky a jejich odpověď na první otázku zněla: *„Nejčastěji se jedná chybu v zabezpečení webové prezentace, tedy nedostatečné aktualizace. Měly by být dostatečně zabezpečeny i Open source programy, které jsou používány k rozšíření výsledných programů a tato rozšíření jsou zdarma. Narušitel může využít těchto rozšíření a skrze ně napadnout tu danou webovou prezentaci.“*

Wp neuron na první otázku: *„Jsou to nejčastěji díry v kódu, který je veřejně dostupný (co se týče Open source systému) a provádějí je lidi, kteří mají zájem na zneužití informací z vaší stránky.“*

Za firmu **Forpsi** odpověděli na první otázku následovně: *„Jedná se primárně o získání citlivých údajů, se kterými se pak útočník snaží naložit určitým způsobem (prodat, použít pro diskreditaci apod.) jedná se tedy hlavně o snahu prolomit hesla k databázím pomocí phishingových aktivit (vydávání se např. za*

poskytovatele platební brány se snahou přesměrovat zákazníky na své stránky). Využívají k tomu potom nedostatečné aktualizace.“

Za společnost **eBola** zněla odpověď na 1. otázku: *„Nejčastější chyby bývají v tom, že si uživatelé neaktualizují své instalované redakční systémy.“*

2) Další otázka se týkala způsobu, jakým řeší napadení kybernetickými zločinci? Odpověď od **ONEbit** zněla: *„Pokud se nám pomocí antivirové kontroly podaří dohledat podezřelou aktivitu na webové prezentaci, případně již upravený soubor s nahraným škodlivým kódem v datech účtu, je-li to v našich silách, dané zneaktivníme a v co nejkratší možné době kontaktujeme našeho zákazníka, kterému jsme v případě řešení problému k dispozici.“*

Český hosting: *„Záleží na tom, o jakou aplikaci se jedná. Dále záleží na programátorovi, jakým způsobem ji opraví. Většinou tu aplikaci odstaví, aby mohl analyzovat webovou stránku, chybu odhalit a upravit. Je to otázka na toho, kdo ten web vytvářel, protože to je ten člověk, který ví, jakým způsobem může tu chybu odhalit a opravit.“*

Firma **Bookassist**: *„Snaží se nejprve předcházet takovému druhu napadení především tak, že jsou auditováni na nejpřísnější kontrolu a zabezpečení. Možnost útoků odhadují a kontrolují. Pokud už k útoku dojde, mají přesné pokyny, jak postupovat v rámci GDPR.“*

Na druhou otázku odpověděli z firmy **Savana**: *„Pokud je škodlivá aktivita detekována – musí být v tu chvíli aktivní, není totiž v našich silách procházet tisíce webových prezentací našich uživatelů. V tu chvíli je webová prezentace pozastavena a je kontaktován náš uživatel. Musí být pozastavena z toho důvodu, že může ohrožovat ostatní zákazníky jak u nás, tak i mimo nás. Uživatel je tedy kontaktován, aby mohl danou situaci co nejdříve vyřešit a aby jeho webová prezentace byla co nejdříve spuštěna.“*

Od **Wp neuron** jsem se dozvěděla, že: *„U standartních Open source se to řeší tím, že se přehraje webová prezentace. V případě, že obsahuje nějaké šablony, tak se musí projít ručně i ty a díky tomu lze odhalit, zda obsahují nějaké viry nebo zda byla ta webová prezentace napadena. Ideálně se přehrají nebo*

aktualizují všechny plug-iny a pak je potřeba podívat se do databáze, zda se tam něco nevyskytuje.“

Za společnost **Forpsi**: *„Monitorujeme infrastrukturu jako celek, pokud detekujeme útok směrovaný přímo na konkrétní web, tak se jej snažíme eliminovat a komunikujeme s jeho majitelem. Zabezpečení na úrovni webu má na starosti jeho správce. Naším úkolem je především funkčnost a zabezpečení infrastruktury jako celku (zamezení vstupu neoprávněných osob do datacentra apod.)“*

Firma **eBola** reagovala na druhou otázku: *„Záleží na webové prezentaci, ale nejčastěji se to řeší tak, že se musí celá přehrát. V případě, že obsahuje nějaké šablony, tak i ty se musí všechny projít, abychom odhalili tu zločinnou aktivitu.“*

3) Proto, že je má práce zaměřena na podnikatele v kyberprostoru v oblasti CR, jsem se ptala, jestli mi dokáží říci, u jakých firem je napadení nejčastější.

Odpověď u **ONEbit** byla, že: *„Takovéto záznamy nikterak nevedeme, není tedy možné určit, jaké společnosti bývají napadány nejčastěji.“*

Český webhosting: *„Tuto informaci nemají. Nelze takto obecně říci, která z těch daných webů je častěji napadena a která méně často. K napadení může dojít u kteréhokoli webu a kdykoliv. Napadení není to omezeno tím, čím se web zabývá, co nabízí či provozuje. Útočníci jednoduše hledají na různých adresách chyby, které mohou zneužít ve svůj prospěch a je úplně jedno, u jakého je to poskytovatele. Hledají chyby u domén a pak z nich provádí nelegální činnosti (například rozesílání spamových zpráv apod.). Nesouvisí to nikterak s tím, zda na webové stránce je platební brána nebo jaký je obsah té webové stránky. Jdou opravdu jen po chybách a po místech, kam by se mohli nabourat.“*

I od firmy **Bookassist** jsem se dozvěděla, že *„na oblasti podnikání nezáleží. Citlivá data mají všichni podnikatelé. Jde tedy o to, kde je zabezpečení nejnižší a tím pádem, kterou stránku je pak nejsnazší napadnout.*“

Navazuje odpověď od firmy **Savana**: *„Tuto otázku nelze zodpovědět. Jediná věc, která může ovlivnit napadení je výše zabezpečení, zda je stránka zabezpečená přes certifikát, přes http. Pokud se však ptáte, co je nejčastěji napadené, tak se to odvíjí přímo od té dané aplikace. Nejčastěji, co uživatelé*

používají, jsou Open source redakční systémy (WordPress, Joomla, Drupal). Tyto typy aplikací jsou volně dostupné, jsou zdarma a jsou předpřipravené. Uživatel tím pádem nemusí znát ten programovací jazyk. Avšak tím, že Open source disponuje volně dostupným zdrojovým kódem, je i snadno napadnutelný.“

Společnost **Wp neuron**: *„U velkých firem nejsou Open source systémy, tudíž je horší pro toho narušitele se tam dostat a hacknout tu danou stránku. Spíše jsou hacknuty stránky menších firem, protože ty používají Open source systémy a jejich kód je volně přístupný.“*

Firma **Forpsi**: *„Bohužel na tuto otázku nejsme schopni odpovědět.“*

Poslední dotázanou firmou byla **eBola** a reagovala takto: *„Takto to říct nelze. Odvíjí se to od aktualizací a o kvalitě programů Open source. Záleží, jak je daná webová prezentace vytvořena.“*

4) Poslední otázkou bylo, jak se vyvarovat případnému napadení?

U firmy **ONEbit** mi bylo sděleno, že: *„Pro snížení šance napadení je důležité udržovat aktuálnost redakčního systému a případných pluginů, neukládat hesla na nezabezpečených místech, neinstalovat podezřelé rozšíření webových aplikací apod.“*

Český hosting: *„Je hlavní, aby byly všechny využívané aplikace aktuální. Pak je minimální riziko, že by se tam mohl kdokoli dostat. Ve chvíli, kdy vyjde nová aktualizace toho webu, tak ji ihned provést. Nové aktualizace totiž opravují chyby těch předchozích verzí aplikací a předcházejí problémům s napadením webových stránek. Hlavní tedy je, aby vše bylo aktuální a zabezpečené.“*

Z firmy **Bookassist** se mi dostalo odpovědi, že *„nejlepší způsob, jak se vyvarovat napadení je neustále vyvíjet a aktualizovat aplikace sloužící k zabezpečení.“*

U firmy **Savana** mi bylo sděleno, že: „*Základem jsou tři úrovně zabezpečení – uživatel si musí zabezpečit svou webovou prezentaci, také své zařízení, prostřednictvím kterého se poté připojuj. Poslední úrovní zabezpečení je vhodný výběr poskytovatele služeb. Dále neukládat hesla v prohlížeči ani nezůstávat*

přihlášen. Ve chvíli, kdy se vir dostane do webové prezentace, dokáže vyčíst všechna uložená hesla a ty pak zneužije ve svůj prospěch. Mít solidního poskytovatele služeb, vědět jaké má uživatel služby a co přesně chce. Správa vlastního serveru je vhodná ve chvíli, kdy s tím má uživatel zkušenosti. Ve chvíli, kdy tyto zkušenosti nemá a stará se o více věcí zároveň, může vzniknout prostor pro napadení.“

Zástupce společnosti **Wp neuron** mi odpověděl: *„Omezit množství Open source systémů, které nejsou ověřeny. Omezit se na vytváření funkcionalit pomocí určitých plug-inů. Také jsou důležité aktualizace. Čím méně aktualizujete, tím je větší riziko, že se někdo dostane k vašim citlivým informacím. Ale neznamená to, že když máte vše aktualizované, že nemůžete mít v PC vir nebo že vám to nemůže nikdo napadnout.“*

Od firmy **Forpsi** se mi dostalo odpovědi: *„Vyvarovat se napadení nelze, lze ale aktivně přistoupit k zabezpečení dat a poradit se s odborníkem na zabezpečení. Také je důležité nepodceňovat zálohování citlivých dat pro možnost obnovy po úniku.“*

Na poslední otázku odpověděli z firmy **eBola**: *„Je důležité používat kvalitní programy, které nejsou snadno napadnutelné, uživatel musí dbát na dané aktualizace. Jsou také programátoři, kteří naprogramují kvalitně, a není pak problém a jsou i tací, kteří to naprogramují špatně a pak je lepší použít redakční systém hotový a vyřešit to zabezpečení prostřednictvím toho systému.“*

Na základě odpovědí od všech sedmi firem jsem došla k závěru, že všechny mnou zmíněné problémy a nástrahy ve virtuálním světě jsou u těchto firem řešeny takřka stejným způsobem. Nejlépe jsou zabezpečeny ty webové stránky, kde se jejich programátoři starají o neustálé aktualizování. Tím totiž eliminuji chyby a nenechávají tak prostor pro útočníky, kteří mají zájem na tom, aby se nabourali do systémů firem a do jejich webových stránek. Když se to nějakému zločinci povede, tak je úkolem programátora, aby nejprve problém analyzoval, napadenou aplikaci odstavil a poté vyřešil daný problém. Následně je třeba informovat majitele webové stránky o provedených úkonech. Jediná firma, u které se odpovědi trošku lišily, byla firma

Bookassist. Jelikož je tato firma zaměřena především na rezervační systémy a komunikoval se mnou Online Business Manager, tak mi odpovídali na mé otázky z jiného hlediska než zbylých šest dotázaných. Poskytnuté odpovědi se však výrazně nelišily od firem ONEbit, Český hosting, Savana, Forpsi, WP neuron a eBola. Tím pádem mohu jejich odpovědi označit za téměř totožné.

Z rozhovorů se zástupci webhostingových firem jsem se dozvěděla, že není žádná spojitost se zaměřením webové stránky a náchylností na kybernetická napadení. Není možné říci, které firmy podnikající v kyberprostoru v oblasti cestovního ruchu jsou nejnáchylnější na kybernetická napadení. Na tomto závěru se shodly všechny firmy a vysvětlili mi, že napadenými stránkami bývají právě ty, které nejsou pečlivě spravovány a tím pádem ani dostatečně chráněny před útoky kybernetických zločinců. Pokud se bavíme o tom, kdo napadá webové stránky, může se jednat buďto o samotné osoby provádějící nelegální činnost nebo o roboty, kteří jsou naprogramovaní k provádění škodlivých činnosti. V poslední otázce jsem se ptala na to, jak předcházet problémům, ale tato otázka byla ve většině případů zodpovězena už v první otázce a tedy, že se dá předcházet útokům neustálou aktualizací aplikací a neustálou kontrolou systémů. Možnému napadení lze také předejít pomocí chráněných redakčních systémů.

2.5 Výzkumná část 3

Poslední část výzkumu je založena na dotazníkovém šetření, kdy jsou respondenty zákazníci, kteří nakupují služby/produkty v oblasti cestovního ruchu. Metodou šetření byl online dotazník vytvoření pomocí Formuláře Google. Šíření online dotazníku bylo uskutečněno pomocí emailových zpráv, aplikace Whats App a také pomocí sociální sítě Facebook.

2.5.1 Charakteristika respondentů

Při výběru respondentů bylo klíčové, aby respondenti patřili mezi uživatele kyberprostoru. Z tohoto důvodu byl dotazník tvořen v online (elektronické) formě. Tím pádem bylo rovnou vyloučeno, že se na dotazníkovém šetření nebudou podílet respondenti, kteří nejsou uživateli kyberprostoru a nepohybují se v něm.

2.5.2 Použité druhy otázek

Online dotazník obsahuje 14 otázek, které jsou uzavřené, polootevřené i otevřené. Převažují však otázky uzavřené, a to s počtem 9 otázek. Polootevřené otázky jsou 3 a otevřené 2. Dotazník je uveden úvodním textem. V textu je respondent seznámen s důvodem tvorby dotazníku, s tématem a obsahem dotazníku. Na konci je představen cíl dotazníkového šetření.

Otázky, které byly použity v dotazníku, jsou seřazeny od otázek týkajících se nákupního chování zákazníků, zda nakupují produkty/služby cestovního ruchu, přes otázky ohledně preferovaného způsobu platby za daný produkt/službu. Další otázky byly zaměřené na téma hrozby v kyberprostoru, obavy z nich a vlastní zkušenosti. Na konci dotazníku jsou doplňující sociodemografické a socioekonomické otázky. Struktura dotazníku:

1) Nákupní chování
2) Způsoby platby
3) Hrozby v kyberprostoru
4) Sociodemografické a socioekonomické otázky

2.5.2.1 Nákupní chování

V této části dotazníku je pouze jedna otázka, která se zabývá nákupním chováním zákazníků a je zaměřena na produkty/služby cestovního ruchu. Pomocí této otázky dokážeme selektovat zákazníky, kteří nakupují produkty/služby cestovního ruchu a tím pádem i zacílit na vzorek respondentů, jejichž odpověď je relevantní pro tento výzkum. V případě, že na ni odpoví negativně, pak postupují rovnou k otázkám sociodemografickým a socioekonomickým.

Otázka:

Nakupujete na internetu jízdenky/letenky/ubytování/zájezdy/pojištění?

Jedná se stručně o produkty/služby CR – raději jsem je ale vypsala, aby respondenti věděli, na co se jich přesně ptám.

2.5.2.2 Způsob platby

U otázek, které jsou zacíleny na způsob platby, odpovídá respondent na tři otázky. Při placení online musí zákazník zadat své platební údaje a mnohdy i osobní údaje, které mohou být zneužity. Je tedy určitý předpoklad, že budou ochotni platit pouze na ověřených stránkách, kde mohou mít jistotu, že je kyberneticky zabezpečená nebo se jedná o stránky, které v nich tento dojem vyvolávají. V této části dotazníku jsou použity otázky uzavřené.

Otázky:

Platíte za nákup výše zmíněných produktů online?

Jakým způsobem platíte nejčastěji v případě nákupu online?

Za jakou službu z následujících nejčastěji platíte online?

2.5.2.3 Hrozby v kyberprostoru

Tento druh otázek je součástí dotazníku z důvodu zjištění informovanosti zákazníků o hrozbách v kyberprostoru. Také jsou zde otázky na zákazníky, zda mají osobní zkušenost se zneužitím údajů při platbě online. Tyto otázky nám podají zpětnou vazbu o tom, jakou mají respondenti zkušenost s platbou online a odpovědi nám pomohou dostat se k jádru problematiky, tedy míra zabezpečení webových stránek firmami/společnostmi podnikajícími v oblasti cestovního ruchu.

Otázky:

O jakých hrozbách při platbě online víte?

Máte nějaké obavy při platbě online (platba kartou online, bankovní převod)?

Pokud ano, čeho se nejvíce obáváte?

Máte Vy osobně nějakou negativní zkušenost při platbě online?

Pokud jste odpověděl/a ano, o jakou zkušenost se jedná?

2.5.2.4 Sociodemografické a socioekonomické otázky

V posledním okruhu otázek byly zjišťovány informace týkající se pohlaví, věku, místa bydliště podle množství obyvatel a také podle kraje, a to u sociodemografických otázek. K socioekonomické otázce patří otázka zaměřená na nejvyšší dosažené vzdělání.

Otázky:

Uveďte prosím Vaše pohlaví.

Uveďte prosím Váš věk.

Jaké je Vaše nejvyšší dosažené vzdělání?

Uveďte prosím místo Vašeho bydliště.

Z jakého kraje pocházíte?

2.5.3 Výsledky výzkumné části 3

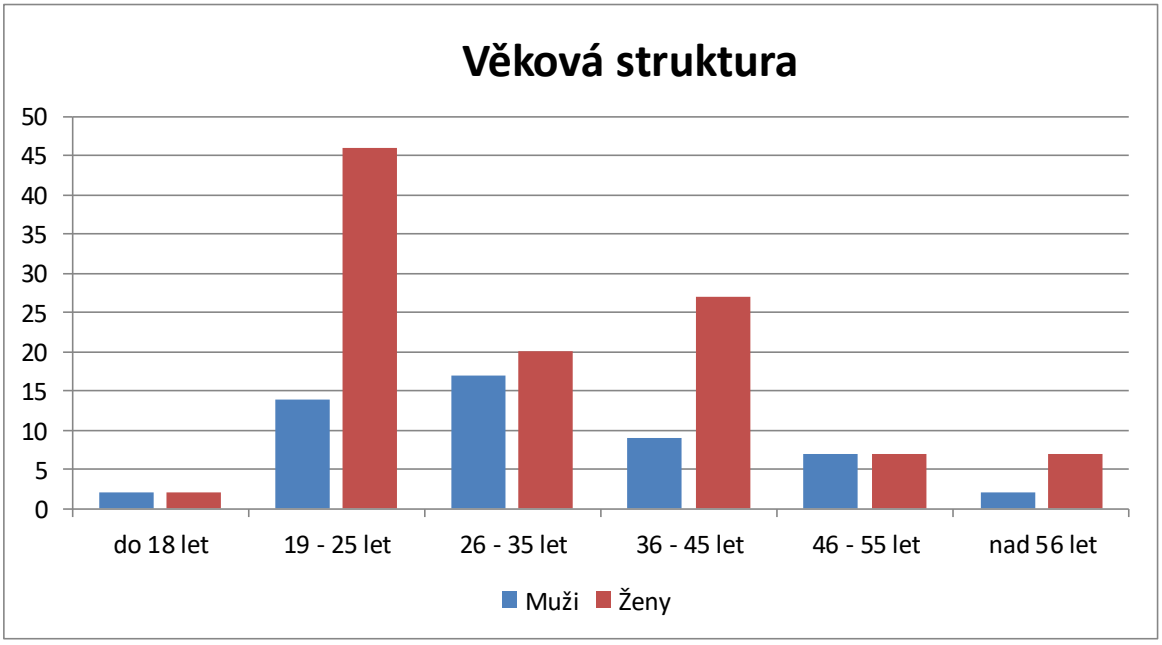
Hlavním cílem tohoto dotazníku bylo zjistit povědomí dotázaných o hrozbách v kyberprostoru a spojitost povědomí o hrozbách a nákupního chování zákazníků. Třetí výzkumnou část jsem provedla kvůli tomu, abych získala pohled na dané téma ze všech tří stran. Nejprve tedy z podnikatelského hlediska, poté z hlediska zabezpečení kyberprostoru skrze externí firmu a nyní z hlediska zákazníků využívající kyberprostor pro nakupování online.

Sociodemografické údaje

Začneme tedy nejprve s celkovým počtem respondentů a sociodemografickými údaji. Celkový počet dotázaných je 160 (100 %) a z toho 109 žen a 51 mužů. Poměr je 68,1 % ku 31,9 %.

Co se týče věkových skupin, tak převažující část respondentů byla ve věku 19-25 a to 37,5 %. Druhou nejčetnější skupinou byli respondenti ve věku 26-35 (23,1 %) a věková skupina 36-45 (22,5 %). 8,8 % respondentů bylo v rozmezí 46-55 let. Nejmenší zastoupení má věková skupina do 18 let (2,5 %) a nad 56 let (5,6 %). Mezi těmito výsledky jsou i 4 respondenti (2,5 %), kteří jsou z věkové skupiny nad 56 let a nenakupují online. Tím pádem je pouze 3,1 % zákazníků, kteří jsou v této věkové

skupině a nakupují online služby v CR. Tyto výsledky poukazují na fakt, že nejčastěji nakupují online zákazníci ve věku od 19-25 let. Snažila jsem se ve výzkumu oslovit všechny věkové kategorie, abych zjistila, jestli lidé v každém věku nakupují online. Díky tomu jsem se dozvěděla, že se ve virtuálním světě nejčastěji pohybují lidé ve věkovém rozmezí 26-45 let. V následujícím grafu můžeme vidět zastoupení mužů a žen v různých věkových skupinách.

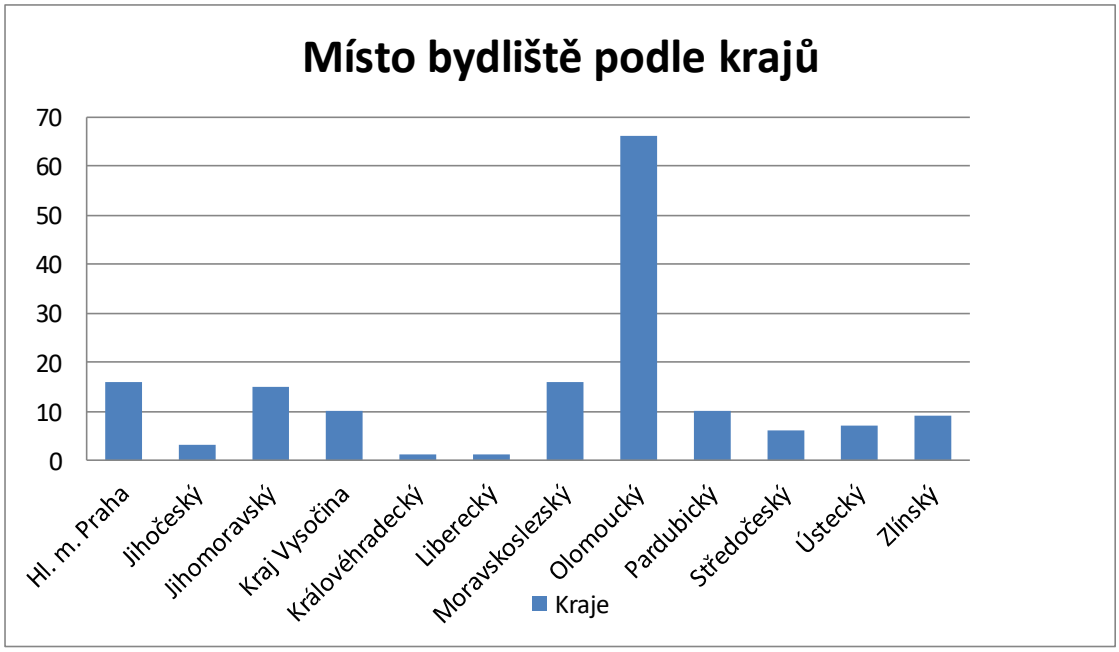


Graf 4: Výzkumná část 3 – Věková struktura respondentů
(Zdroj: vlastní zpracování)

Na základě otázky na místo bydliště respondentů jsem se dozvěděla, že 26,9 % respondentů pochází z vesnice do 2 000 obyvatel. Větší část (13,1 %) pak pocházela z měst s 100 001 – 200 000 obyvateli. 11,3 % respondentů žije ve městě mezi 50 001 – 100 000 obyvateli a s obyvateli nad 500 001. Méně jak 10 % procenty jsou pak zastoupeny města s 2 001 – 50 000 obyvateli a 200 001 – 500 000 obyvateli.

Z pohledu krajů je nejvíce zastoupen Olomoucký kraj a to s 41,3 %. S 10 % jsou pak zastoupeny kraje Moravskoslezský a hlavní město Praha. 9,4 % respondentů je z Jihomoravského kraje. Zbytek respondentů je z krajů: Vysočina, Pardubický, Ústecký, Zlínský, Středočeský, Jihočeský, Liberecký a Královéhradecký. Kraje Plzeňský a Karlovarský nejsou zastoupeny vůbec. Snažila jsem se obsáhnout respondenty z co nejvíce krajů, což se mi povedlo díky tomu, že jsem svůj dotazník šířila v níže

zmíněných krajích. Následující graf přehledně znázorňuje rozdělení respondentů podle krajů, ze kterých pocházejí.



Graf 5: Výzkumná část 3 – Místo bydliště podle krajů

(Zdroj: vlastní zpracování)

Socioekonomické údaje

Socioekonomická otázka byla v dotazníku pouze jedna a byla zaměřena na nejvyšší dosažené vzdělání respondentů. Nejvíce respondentů má Střední školu s maturitou (35%). Dále byla nejčetnější odpověď Vysoká škola (titul Mgr., Ing., MUDr., JUDr.) 26,2 % a Vysoká škola (titul Bc.) 25 %. Respondentů se Středním odborným učilištěm bez/s maturitou, anebo Vyšší odbornou školou bylo nejméně, a to pouze mezi 3-5 %.

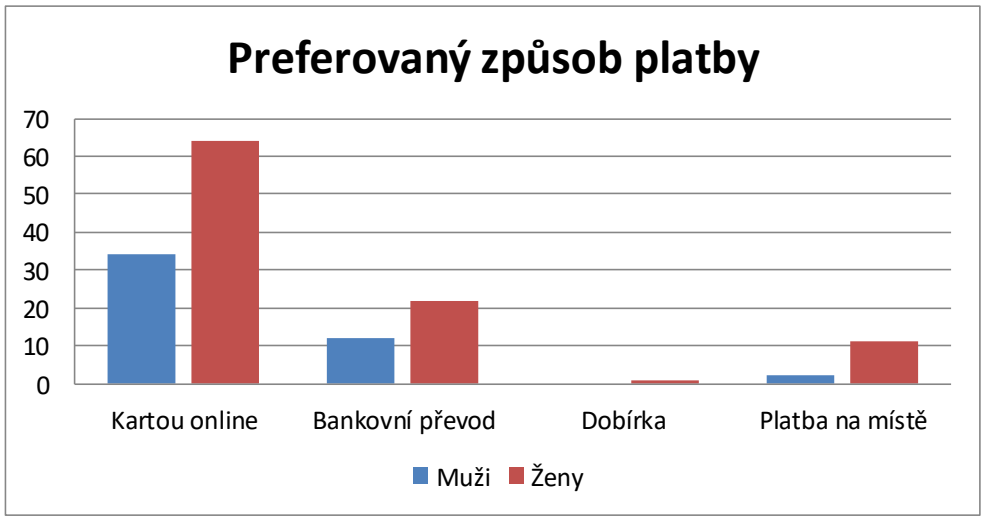
Nákupní chování

Následuje otázka, která byla zaměřena na nákupní chování zákazníků a zněla: Nakupujete na internetu jízdenky/letenky/ubytování/zájezdy/pojištění? Z celkových 160 dotázaných odpovědělo 146 (91,3 %), že ano. Zbylých 14 respondentů (8,8 %) zaškrtlo možnost druhou, tedy že nenakupují tyto produkty online. Těchto 8,8 % respondentů

bylo tedy hned přesměrováno na otázky sociodemografické a socioekonomické a dále nebyli zahrnuti v ostatních otázkách.

Způsob platby

Další okruh otázek, který je zaměřen na způsob platby při nákupu na internetu začíná otázkou, zda platí respondenti za nákup výše zmíněných produktů (jízdenky/letenky/ubytování/zájezdy/pojištění) online. Z celkového počtu 146 respondentů odpovědělo 92,5 %, že platí online a pouhých 7,5 %, že ne. Následovala otázka, jakým způsobem tedy platí nejčastěji při nákupu na internetu. U této otázky odpovědělo 99 respondentů, že upřednostňují platbu kartou online – z toho 64 žen a 34 mužů. 34 zákazníků preferuje platbu bankovním převodem (22 žen a 12 mužů). Platbou na místě (pokud možno) pak preferuje zaplatit 12 dotázaných z toho 11 žen a 2 muži. Byl zde prostor i pro vlastní odpověď a tuto možnost zvolil 1 respondent (žena) odpověděl, že upřednostňuje platbu na dobírku. Na základě těchto údajů je vyhotoven graf číslo 6, kde můžeme vidět výše uvedené hodnoty.

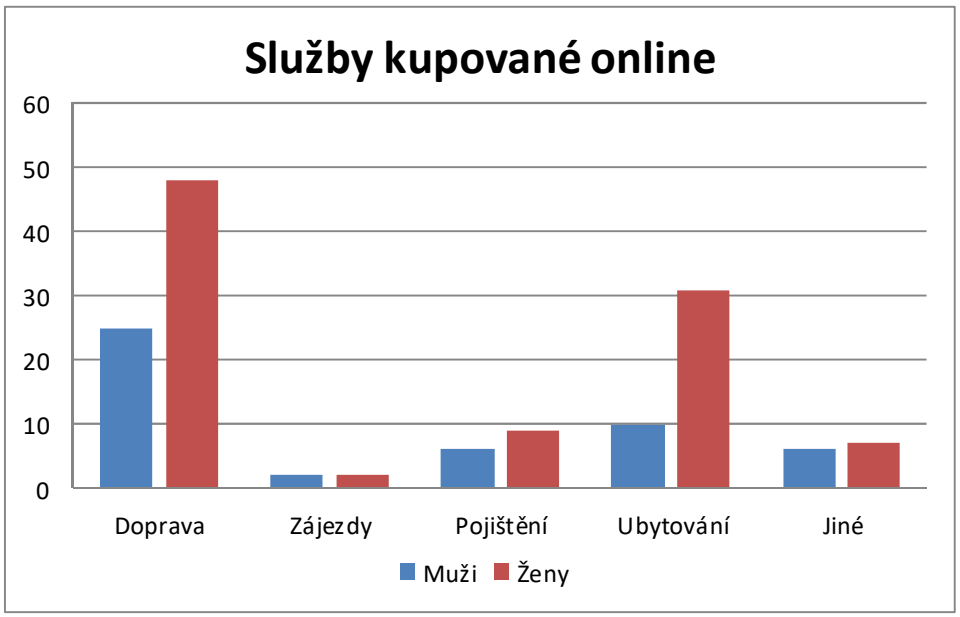


Graf 6: Výzkumná část 3 – Preferovaný způsob platby při nákupu online

(Zdroj: vlastní zpracování)

Proto, že je tato práce zacílena na cestovní ruch, tak mne zajímalo, za co lidé nejčastěji v tomto okruhu služeb platí online. A to byla také moje následující otázka. Nejčastější odpovědí byla doprava a zvolilo ji 73 dotázaných. Druhou nejčetnější skupinou byli ti zákazníci, kteří nejčastěji platí online za ubytování. Ubytování zvolilo 41 lidí. Následovalo pojištění, které online nakupuje 15 zákazníků. Nejméně zákazníci nakupují

zájezdy. Tuto možnost zvolili pouze 4 respondenti. Zbylých 13 dotázaných odpovědělo, že nejčastěji platí online za jiné než zmíněné produkty. Ty se nevztahovaly k cestovnímu ruchu, a tudíž je zde nebudu uvádět. V grafu 7 jsou znázorněny pod názvem Jiné. (doprava – 48 žen, 25 mužů), (zájezdy – 2 ženy, 2 muži), (pojištění – 9 žen, 6 mužů), (ubytování – 31 žen, 10 mužů), (jiné – 7 žen, 6 mužů).

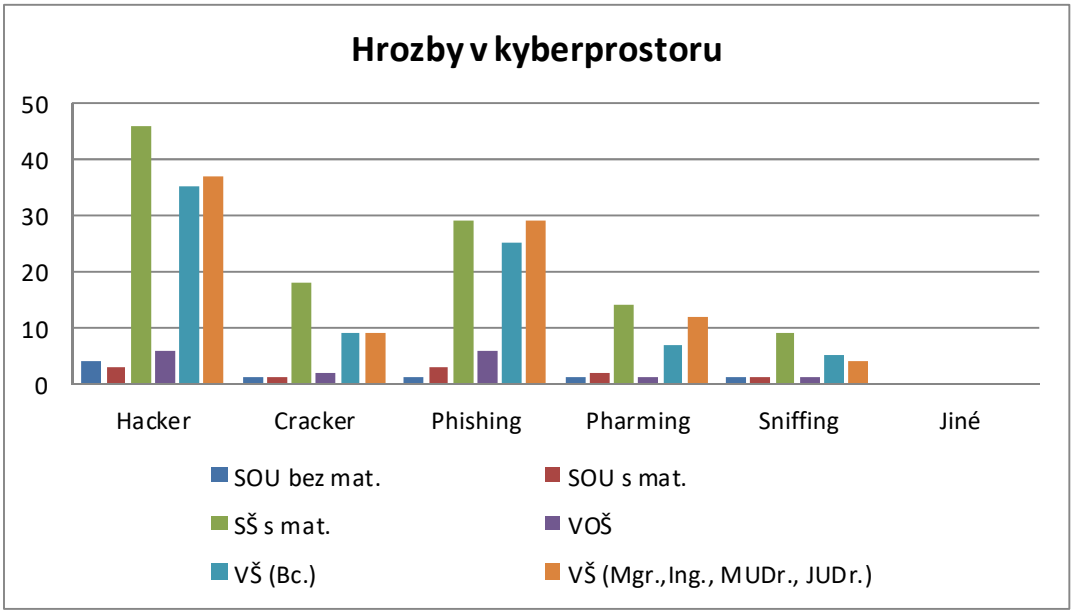


Graf 7: Výzkumná část 3 - Služby kupované online

(Zdroj: vlastní zpracování)

Hrozby v kyberprostoru

Poslední okruh otázek třetího výzkumu jsou otázky na téma hrozby v kyberprostoru. Pro téma mé bakalářské práce je stěžejní dozvědět se, jaké informace má veřejnost o hrozbách ve virtuálním světě a jak na ně nahlíží. První otázka zněla: O jakých hrozbách při platbě online víte? Na výběr bylo 5 možností: Hacker, Cracker, Phishing, Pharming a Sniffing. Respondenti měli možnost zvolit více než jednu odpověď a měli možnost doplnit svou vlastní odpověď v případě, že nebyla mezi vypsanými. Dotázaným bylo také vysvětleno, co jaký pojem znamená. Nejvíce respondentů zaškrtlo, že znají nebo už někdy slyšeli pojem Hacker (92,5 %) a Phishing (64,4 %). Výrazy Cracker a Pharming jsou známy jen 27 % dotázaných. Nejméně známý pro ně byl pojem Sniffing. Slyšelo o něm pouze 15,1 % z respondentů, což můžeme vidět na další straně v grafu číslo 8.

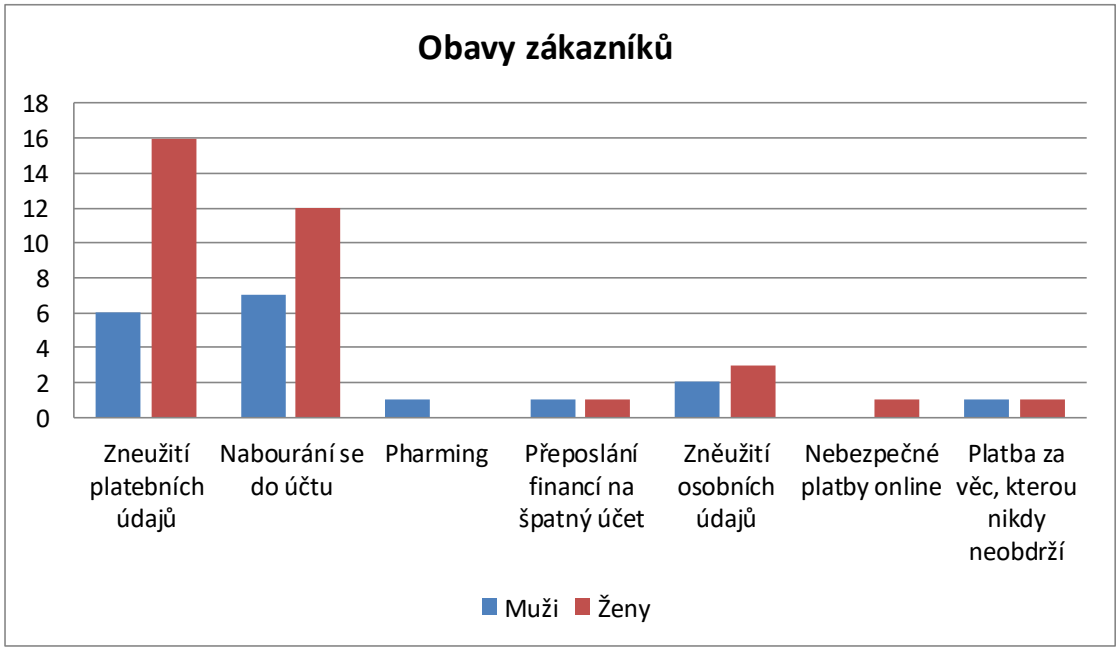


Graf 8: Výzkumná část 3 - Hrozby v kyberprostoru
(Zdroj: vlastní zpracování)

Navazuje otázka, zda mají respondenti jako zákazníci nějaké obavy při platbě online. Pro 59,6 % dotázaných platí, že nemají obavy při platbě kartou online nebo při platbě uskutečněné bankovním převodem. Zbytek respondentů, tedy 40,4 % obavy mají. Tyto výsledky, kde větší část dotázaných odpověděla, že obavy nemají, mohou poukazovat na fakt, že se většina zákazníků osobně, ani prostřednictvím lidí v jejich okolí, nesetkala s žádným problémem při placení online. Může to být ale také z toho důvodu, že nejsou dostatečně informováni o hrozbách, které se ve virtuálním světě vyskytují. Na druhé straně, respondentů, kteří odpověděli, že strach mají, je téměř polovina. Mohou to být zákazníci, kteří se buďto setkali s nějakými hrozbami, nebo o nich slyšeli od uživatelů ve svém okolí. Anebo jsou to uživatelé, kteří jsou informováni o možných hrozbách. Například lidé, kteří se v tomto odvětví orientují a jsou si vědomi všech možných rizik internetu a placení jeho prostřednictvím.

Respondenti, kteří odpověděli, že mají obavy při platbě online, měli možnost odpovědět v následující otevřené otázce, čeho se obávají. Na tuto otázku odpovědělo 52 respondentů a mezi odpověďmi byly převážně dvě hlavní odpovědi. Buďto se dotázaní obávají zneužití platebních údajů, anebo že jim budou zcizeny všechny peníze, které mají na účtu. Bojí se také toho, že stránka, na které chtějí platbu provést je falešná – tedy Pharmingu. Mezi další odpovědi patřily ty, že mají strach z toho, že pošlou peníze na špatný účet, že zaplatí za danou věc, ale ta jim nikdy nedojde. Bojí se

nezabezpečených plateb online, které přímo souvisí se zabezpečením webových stránek poskytovatelů. Veškeré obavy, které mají zákazníci při platbě online, jsou přehledně znázorněny v grafu číslo 9.

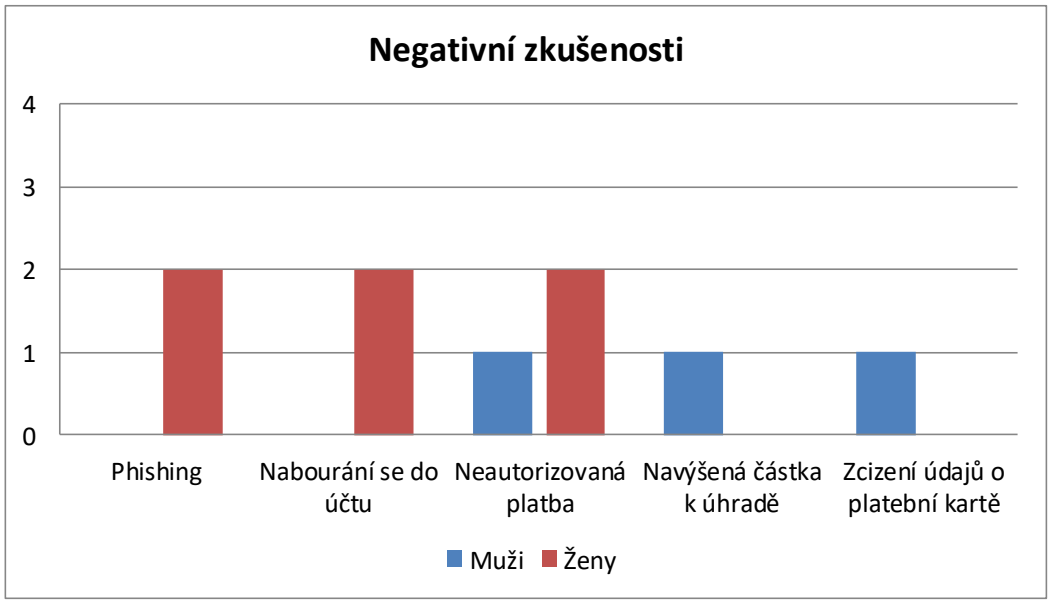


Graf 9: Výzkumná část 3 - Obavy zákazníků
(Zdroj: vlastní zpracování)

V další otázce jsem se ptala dotázaných, zda mají osobní negativní zkušenost například se zneužitím platebních údajů. Kladně mi na tuto otázku odpovědělo pouze 9 respondentů. Zbylých 93,9 % zákazníků tuto zkušenost nemá, což je velmi dobrá zpráva.

Ti, kterým však byly údaje zneužity, měli možnost v následující otevřené otázce odpovědět, o jakou zkušenost se přesně jednalo. Dva z respondentů mají přímou zkušenost s Phishingem, což znamená, že se útočník vydával za banku a požadoval provedení určité operace (např. kliknout na přiložený odkaz). Na základě toho se jim naboural do účtu a s tím mají zkušenost další dva respondenti. Další zkušeností je neautorizovaná platba. Toto se stalo dalším třem respondentům, přičemž u dvou z nich se jednalo o neautorizovanou platbu ze zahraničí. Další respondent uvedl, že při platbě kartou online mu bylo strženo místo 25 dolarů rovnou celých 225 – tedy o 200 dolarů více. Poslední zkušenost se zneužitím měla respondentka, u které si útočník opsal údaje o kartě a poté prováděl platby online pod 500Kč (u takto malých částek není vyžadováno potvrzení kódem). Čtyři z devíti respondentů také uvedl, že jim banka

vrátila peníze zpět poté, co respondenti tuto skutečnost nahlásili. Z grafu 10 můžeme vyčíst, s jakou negativní zkušeností mají respondenti dle pohlaví nejčastější zkušenost.



Graf 10: Výzkum č. 3 – Negativní zkušenosti respondentů
(Zdroj: vlastní zpracování)

2.6 Srovnání firem poskytujících webhosting

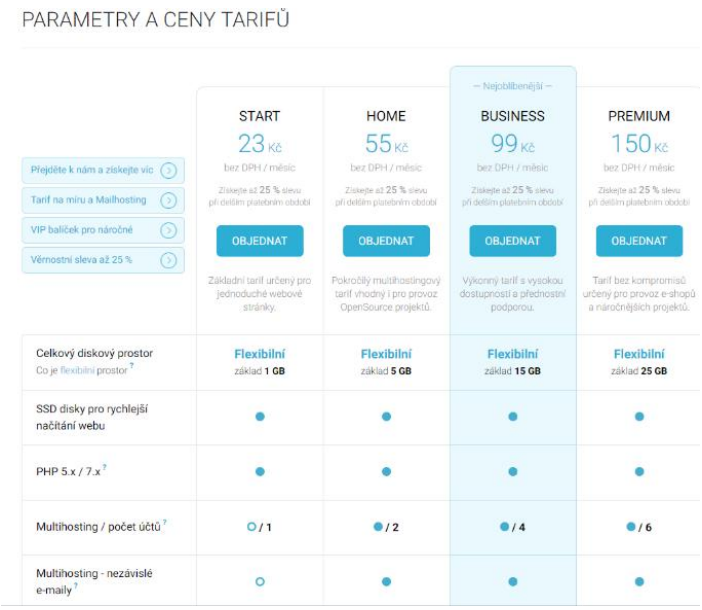
Na základě výsledků především z prvních dvou výzkumů jsem vyhotovila následující tabulku. V tabulce je 5 webhostingových firem, které by mohly být pro podnikatele nejzajímavější, co se nabízených služeb týče.

Tabulka 3: Srovnání webhostingových firem

Logo	Měsíční cena bez DPH	Prostor pro web	Počet emailových účtů	Zálohování	Profesionální podpora
onebit hosting	99,-	10 GB	∞	1x týdně + individuálně	Tel. (9-17), email, online chat
český hosting	83,-	10 GB	∞	Denně	PO-PÁ (8-23) telefon, online chat, email
savana WEBHOSTING	90,-	20 GB	∞	1x za 2 dny	PO-PÁ (8-22) SO-NE (9-12) telefon, online chat, email
forpsi INTERNET CZ, a.s.	80,-	∞	∞	Denně	24/7 telefon, online chat, email
Hosting WEDOS	70,-	∞	∞	1x týdně	24/7 online chat, email

(Zdroj: vlastní zpracování)

Na první místo jsem zařadila firmu ONEbit pro jejich výhody, mezi něž patří například bezplatná zkušební doba 2 měsíce, dobrá dostupnost a pohotová podpora. Také jejich webové stránky jsou přehledné a díky tomu rychle najdete přesně to, co hledáte. Sami sebe hodnotí jako nejlepší hosting v poměru ceny a výkonu. Nabízí více balíčků, díky kterým si na své přijde každý. Viz obrázek níže.



2. Obrázek: Druhy tarifů od firmy ONEbit

Zdroj: Onebit.cz, 2018

Pro tarif business, jehož hodnoty jsou zaznamenány v tabulce, platí také přednostní zákaznická podpora, což podnikatelé jistě ocení. ONEbit je hodnocena jako nejdostupnější webhostingová firma v ČR a v roce 2018 byl vyhodnocen jako nejlepší hosting mezi 17 předními webhostery v ČR. Jedinou nevýhodou u ONEbit je zákaznická podpora, která nefunguje non-stop. Na telefonickou linku se mohou zákazníci dovolat od 9-17 hod nebo mají možnost využít emailovou zprávu či online chat.

Druhé místo obsadil Český hosting, který nabízí bezplatnou zkušební dobu 14 dní a garanci vrácení platby do 30 dnů. Všechny služby nabízí v jednom druhu tarifu za neměnnou cenu. Nelze si tedy pořídit tarif o třídu vyšší, což ale není na závadu. Jediný nabízený tarif se vyrovná vyšším tarifům nabízených konkurencí. Také má přehledné webové stránky, na kterých rychle naleznete veškeré potřebné informace. Denně jsou

data zálohována a přístupna. Další kladnou stránkou Českého hostingu je ochotná a odborná podpora. Ta však není 24/7, stejně jako u firmy ONEbit. Mezi zápory bych zařadila diskový prostor (parametr určující velikost pronajatého prostoru), který může být pro určité společnosti malý a za jeho navýšení si musí podnikatel připlatit.

Na třetím místě je webhostingová firma Savana. Mezi její výhody patří garance vrácení peněz do 30 dnů. Také jejich webové stránky jsou přehledné a nehrozí, že byste se v nich ztratili. Nabízí dva tarify: Savana 101 a Savana 201. Viz obrázek níže vidíme rozdíly mezi levnější a dražší variantou.

3. Obrázek: Druhy tarifů od firmy Savana

Zdroj: Savana.cz, 2018

Pokud se podíváme na zápory u firmy Savana, tak to bude jistě zákaznická podpora, která taktéž není 24/7. V případě nutnosti však funguje dopoledne mezi 9-12 hodinou o víkendu a taktéž i ve státních svátcích. Nevýhodou také může být zálohování, které je prováděno jednou za dva dny.

Čtvrté místo patří firmě Forpsi, která disponuje přehlednými stránkami. Nabízí bezplatnou 18 – ti denní zkušební dobu a je vlastníkem SSL certifikátů. „*SSL jsou protokoly, které při správném používání dělají servery a internet bezpečnějším. Zaručují*

identifikaci, tudíž má klient i server jistotu, že komunikují spolu navzájem, a ne s někým, kdo se za jednu ze stran pouze vydává. Zároveň zajišťují šifrování komunikace a tím zařídí bezpečnou výměnu klíčů, které pak klient i server používají právě k šifrování jejich komunikace."[13] Další velkou výhodou u firmy Forpsi je, že pro zákazníky je podpora, ve formě zákaznické linky i emailové komunikace, dostupná non-stop. Stejně jak u firem ONEbit a Savana, i Forpsi nabízí různé varianty hostingů. Viz obrázky níže.

	Varianta hostingu		
	Easy	Advanced	Professional
DV SSL Certifikát	✓	✓	✓
Velikost prostoru pro web	∞	∞	∞
Počet emailových schránek v ceně	∞	∞	∞
Přenos dat (traffic)	∞	∞	∞
FTP / FTP SSL	✓	✓	✓
+ Aplikace			
ASP / ASP.NET / PHP	✓	✓	✓
Aliasy v ceně	5	10	15
Databáze v ceně	1	2	5
Subdomény v ceně	5	5	5
GIGA mail v ceně	5	5	5

4. Obrázek: Druhy tarifů od firmy Forpsi (1)

Zdroj: Forpsi.com, 2018

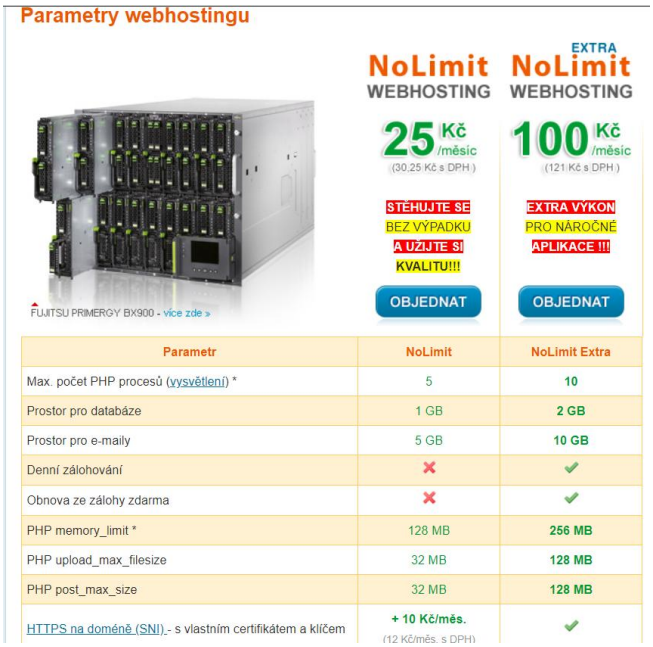
GIGA mail v ceně	5	5	5
Max. velikost schránky	10 GB	20 GB	30 GB
Statistiky návštěvnosti	-	✓	✓
Zálohy webu	✓	✓	✓
Zákaznická podpora 24/7	✓	✓	✓
BUSINESS mail v ceně	✓	✓	✓
Cena za měsíc	od 40,- Kč (48.40 s DPH)	od 80,- Kč (96.80 s DPH)	od 120,- Kč (145.20 s DPH)
	Více info	Více info	Více info
	Objednat	Objednat	Objednat

5. Obrázek: Druhy tarifů od firmy Forpsi (2)

Zdroj: Forpsi.com, 2018

[13] https://www.master.cz/blog/co-jsou-ssl-certifikaty-a-ssl-protokoly-jak-funguji-vysvetleni-navod/

Na pátém místě v tabulce je firma Wedos. Mezi její klady patří zkušební doba 7 dní. Garantují vrácení peněz až do 180 dnů, což nenabízí žádná z výše uvedených firem. Také je nejprodávanější hostingovou společností v letech 2011-2018. V těchto letech je nejprodávanější pro webový hosting za nejnižší ceny. V rámci svých tarifů nabízí jako bonus zdarma vyhotovení statistik návštěvnosti daných webových stránek.



Parametr	NoLimit	NoLimit Extra
Max. počet PHP procesů (vysvětlení) *	5	10
Prostor pro databáze	1 GB	2 GB
Prostor pro e-maily	5 GB	10 GB
Denní zálohování	✗	✓
Obnova ze zálohy zdarma	✗	✓
PHP memory_limit *	128 MB	256 MB
PHP upload_max_filesize	32 MB	128 MB
PHP post_max_size	32 MB	128 MB
HTTPS na doméně (SNI) - s vlastním certifikátem a klíčem	+ 10 Kč/měs. (12 Kč/měs. s DPH)	✓

6. Obrázek: Druhy tarifů od firmy Wedos

Zdroj: Hosting.wedos.com, 2018

Firma Wedos se také pyšní téměř 100 % zabezpečením. Také jejich zákaznická podpora je 24/7, ale pouze ve formě emailů, online chatu a kontaktního formuláře. Nevýhodou u Wedosu je nemožnost spojit se s firmou telefonicky. Zálohování je prováděno pouze 1x týdně a mají opakované potíže s dostupností.

2.7 Diskuze

Bakalářská práce je zaměřená na zabezpečení a hrozby v kyberprostoru ohrožující podnikatele při práci v něm, a to především na prodeje služeb/produktů online. Nejprve jsem uvedla definice nezbytné pro pochopení tématu a poté jsem zkoumala, jakými způsoby se podnikatelé chrání před hrozbami skýtající práce ve virtuálním světě. Slovácký deník zveřejnil v září 2018 článek, který nese titulek „Kyberkriminalita na Slovácku: firmu chtěl připravit o osm tisíc euro“. Článek seznamuje čtenáře s podvodným jednáním vůči firmě, kdy pachatel odeslal nejmenovanému zaměstnanci email, který obsahoval potvrzení údajů k navýšení kapacity schránky. Ve chvíli, kdy příjemce zprávy potvrdil pár kroky požadované údaje, získal pachatel přístup k emailům firmy, která v té době komunikovala se zahraničním partnerem. Zprávy s partnerem obsahovaly fakturační údaje, které pachatel zaměnil, a na pozměněný účet byly poslány požadované finance. (Slovacky.denik.cz, [online], 2018) Takovýchto případů je každým rokem čím dál více, a proto je nutné, aby se firmy chránily. Podle iRozhlasu je terčem útoku každá třetí firma v Česku. Společnost PwC přitom uvádí, že se v posledních dvou letech stalo obětí více než 30 procent tuzemských firem. Nejvíce útoků pak zaznamenávají finanční a výrobní odvětví a firmy z oboru energetiky. (irozhlas.cz, [online], 2018) Pro moji práci je sice potěšující zjištění, že vybrané firmy v cestovním ruchu nejsou těmi nejčastěji napadenými, ale z mého výzkumu vyplývá, že nelze firmy v CR jednoduše vyřadit ze seznamu napadených firem. Nezáleží totiž tolik na odvětví, ve kterém firma podniká, ale na formě a míře zabezpečení a také na příležitostech pro zločince k trestné činnosti.

Dle internetového magazínu Česká pozice deníku Lidové noviny vzrostla kyberkriminalita v České republice za posledních sedm let téměř čtyřnásobně. Tyto údaje uvedli na svém serveru v květnu roku 2018. Uvedli také, že nejčastějším trestným činem na internetu je podvod, který bývá nejčastěji proveden ve formě phishingu [útočník se vydává za banku a požaduje provedení určité operace (např. kliknout na přiložený odkaz)]. (Ceskapozice.lidovky.cz, [online], 2018) I z tohoto důvodu jsem provedla třetí výzkumnou část, která je zaměřena právě na uživatele pohybující se v kyberprostoru, a ve které jsem zjišťovala jejich povědomí o hrozbách vyskytujících se ve virtuálním světě. Fakt, že phishing je nejčastější podvodnou metodou podporuje i článek od iRozhlasu. „Nejčastěji se útočník snaží získat citlivé informace v podobě čísel

platebních karet, hesla k účtům a tak dále. Zkušenosti s takovým typem kyberútoku pak hlásí až 41 % firem. Dalším typem útoku pak je vyděračský malware nebo falešné emaily (například od ředitelů společností s příkazem převést určitý obnos na zadaný účet) a podle policejních statistik došlo v roce 2017 téměř k 6500 počítačových útoků, což bylo skoro o 1000 více než v roce 2016.“ (irozhlas.cz, [online], 2018)

Pro svou práci jsem také použila dotazník pro firmy zajišťující webhostingové služby, které pak nabízejí podnikatelům. Tento výzkum jsem vyhotovila, abych se dozvěděla, jak zabezpečení webových stránek funguje, na co dávat pozor a jak se chránit před případným napadením. Tuto část jsem mohla více propracovat a udělat ji obsáhlejší co se kladených otázek týče a tím se dozvědět ještě více o formách zabezpečení a vhodných postupech. Avšak jsem tak neučinila z toho důvodu, že tato práce je zaměřena primárně na podnikatele v CR, a ne na oblast ICT (informační komunikační technologie). Práce, jak jsem již zmínila, obsahuje základní pojmy, které jsou nezbytné pro uvedení do tématu, ale také mohou posloužit jako jakási osvěta a doplnění znalostí čtenářů o hrozbách vyskytujících se ve virtuální realitě. Touto činností se také zaobírá projekt Bezpečný internet.cz, který „oslovuje různé cílové skupiny uživatelů a na názorných příkladech pomáhá vytvářet správné návyky internetové bezpečnosti.“ Do tohoto projektu jsou zapojeny společnosti: Česká spořitelna, Microsoft a Seznam.cz a jejich hlavním cílem je posílení celkového povědomí o rizicích pomocí společných aktivit. Také jim jde o vzdělání českých uživatelů internetu. Poskytují zcela zdarma rady, návody i zkušenosti provozovatelů nejnavštěvovanějších internetových služeb. (Prevencekriminality.cz, [online], 2019)

2.8 Přínos a návrh řešení v praxi

Tato práce byla vyhotovena s cílem představit problematiku kybernetické bezpečnosti a zjistit jakým způsobem podnikatelé zabezpečují své internetové stránky. K naplnění tohoto cíle mi pomohla tři výzkumná šetření. V první řadě se jednalo o dotazník určený pro podnikatele v CR a rozhovor s firmami poskytující webhosting. Následoval dotazník pro zákazníky, díky kterému se mi podařilo plně pochopit důležitost bezpečnosti webových stránek pro jejich majitele.

Výzkum jsem poté doplnila o tabulku firem na českém trhu poskytujících webhosting. Jedná se o srovnání těchto poskytovatelů podle parametrů, které mohou být klíčové pro podnikatele v CR. Má být pomocným nástrojem pro podnikatele, kteří mají v plánu obrátit se na webhostingovou firmu, jaká firma by pro ně mohla být tím nejlepším řešením. Touto kapitolou jsem se tedy dostala k naplnění dalšího cíle mé bakalářské práce.

1) Na základě první výzkumné části jsem se od dotázaných firem dozvěděla, že převážná část využívá externí firmu, která zabezpečuje jejich internetové stránky, a to co se týče webhostingu, tak i celkového zabezpečení. I dle mého názoru se jedná o nejjednodušší, ale také nejspolehlivější způsob pro podnikatele, jak zabezpečit jejich webovou prezentaci. Podnikatelé si mohou vybrat, na kterou firmu se obrátit. Pro usnadnění výběru jsem vyhotovila již zmíněnou tabulku, která se nachází na stránce 48 v kapitole 2.6 *Srovnání firem poskytujících webhosting*. Jedná se zde o 5 webhostingových firem, které jsem srovnala podle ceny, velikosti nabízeného místa pro internetovou stránku, ale také podle kvality zákaznické podpory. Ta je důležitá, protože zákazník (tedy podnikatel) má jistotu, že kdykoli potřebuje pomoc, má se na koho obrátit. Uváděla jsem dále frekvenci zálohování, jež je nepostradatelnou součástí a může být pro podnikatele rozhodujícím faktorem pro výběr dané externí firmy. Firmy mnou uvedené nabízí různé benefity pro své zákazníky, jako jsou například: bezplatná zkušební doba, garance vrácení peněz, SSL protokoly, různé druhy tarifů (klient si může vybrat například ze 2 nebo ze 3 druhů tarifů), anebo vyhotovení statistik návštěvnosti klientovy webové prezentace. Doporučuji tedy obrátit se na specializovanou společnost, která se touto tematikou zaobírá. Toto řešení doporučuji i na základě druhé výzkumné části, a tedy rozhovoru

s webhostingovými firmami, které zmiňují, že předejít případnému napadení můžeme už jen tím, že vložíme svou internetovou stránku do rukou odborníků.

2) Druhým přínosem jsou výsledky z poslední výzkumné části, tedy dotazník pro zákazníky. Na základě jejich odpovědí je jasně čitelná důležitost, kterou kladou na zabezpečení webových stránek, které navštěvují. Téměř polovina respondentů (přesně 40, 4 %) má obavy ze zneužití citlivých údajů či nabourání se do účtu, ke kterým může dojít právě skrze nezabezpečené stránky. Jedná se o informace velmi důležité pro podnikatele právě proto, že na zákaznících stojí celý jejich úspěch a tím pádem je jejich spokojenosti tím stěžejním pro fungování jejich podnikání.

3) Přínosem mé práce je v neposlední řadě také popis, jak předcházet možnému napadení internetové stránky. Na tuto otázku mi odpovídaly webhostingové firmy jejichž zástupci popisovali, jakými způsoby se lze chránit před napadením. Nelze se spoléhat pouze na zabezpečení skrze webhostingovou firmu, ale je nutné, aby sami podnikatelé prováděli preventivní opatření, jako jsou: neukládat hesla a nezůstávat přihlášeni na svých profilech, využívat nově dostupných aktualizací, zálohovat data, také doporučují omezit množství používaných Open source systémů.

4) Dalším návrhem, který může být využit, je vzdělání zaměstnanců. Je velmi důležité, aby zaměstnanci byli vzděláváni a seznamování s možnými hrozbami. Na základě článku uvedeném v diskuzi můžeme vidět, že vzdělávání zaměstnanců není nikdy dost a mnohdy na tom závisí fungování celé firmy. Vzdělávání může probíhat formou kurzů koupených v rámci firmy určené plošně pro všechny zaměstnance. Vzdělávací kurzy nabízí například NCKB (Národní centrum kybernetické bezpečnosti) a pyšní se tím, že jsou první, kteří takovouto vzdělávací aktivitu začali provozovat. Zaměstnanci se mohou vzdělávat a seznamovat se s důležitými informacemi také individuálně, a to prostřednictvím již zmiňovaného projektu Bezpečný internet.cz, kde si mohou uživatelé psát o rady a informace týkající se používání internetu. Ty jim sdělují zcela zdarma poskytovatelé nejnavštěvovanějších internetových služeb – Microsoft, Seznam.cz a Česká spořitelna. Nutnost vzdělávání zaměstnanců podporuje článek internetového deníku Aktuálně.cz, který v roce 2017

informoval o vzrůstajícím kybernetickém nebezpečí. Zmiňuje se o hackerském útoku programu WannaCry, který byl proveden v květnu roku 2017 a zasáhl tisíce počítačů ve 150 zemích světa. Na tuto událost reagovalo O2 konferencí, kde byl hlavní hvězdou legendární hacker Kevin Mitnick a který konstatoval, že: „Nejslabším článkem jsou vždy lidé. Už za vývojem jednotlivých operačních systémů stojí přeci vývojáři, kteří nejsou přirozeně neomylní.“ (Zpravy. aktualne.cz, [online], 2017)

3 Závěr

Cílem bakalářské práce „Kybernetická bezpečnost pro podnikání v kyberprostoru v oblasti cestovního ruchu“ bylo představení problematiky kybernetické bezpečnosti pro podnikání v něm a zjištění, jakým způsobem podnikatelé zabezpečují své internetové stránky. Práce je rozdělena na část teoretickou a praktickou.

V teoretické části jsou uvedeny a popsány základní pojmy týkající se tématu. Nejprve jsou pomocí definic popsány základní pojmy jako kyberprostor, podnikání v kyberprostoru, zabezpečení a hrozby vyskytující se ve virtuální světě. Následně jsou uvedeny formy podnikání v kyberprostoru v oblasti cestovního ruchu, které jsou rozděleny na kategorie podle zaměření jejich podnikání a jsou zobrazeny v tabulce.

Praktická část slouží jako pohled na danou tématiku z pohledu firem podnikajících ve virtuálním světě, z pohledu webhostingových firem zajišťující nejen tvorbu webových stránek, ale i jejich zabezpečení a v poslední řadě i z pohledu uživatelů internetu. Je tedy složena ze tří různých výzkumných šetření.

První částí výzkumu je kapitola 2.3 a jedná se o rozhovor s podnikateli v oblasti CR v kybernetickém prostoru. Na základě odpovědí z prvního rozhovoru jsem pokračovala druhou částí výzkumu v kapitole 2.4, kterou je také rozhovor. Tentokrát byly otázky rozhovoru směrovány na firmy poskytující webhosting a zabezpečení webových stránek. Odpovědi a jejich vyhodnocení se nacházející v kapitole 2.4.3. Posledním výzkumem byl dotazník pro uživatele webových stránek a zákazníky společností poskytující služby a produkty cestovního ruchu. V kapitole 2.5.3 jsou pomocí grafů a jejich detailních popisů znázorněny jejich odpovědi, které mi pomohly pro kompletní vyhodnocení problematiky bezpečnosti webových stránek.

V úplném závěru praktické části se nachází tabulka srovnávající 5 webhostingových firem, které jsem vyhodnotila na základě uvedených parametrů, jako 5 nejvýhodnějších pro podnikatele. Tabulka se nachází v kapitole 2.6 a za tabulkou dále následuje popsání firem a uvedení již zmíněných parametrů, kvůli kterým se umístily na tom daném místě.

Za praktickou částí následuje diskuze, ve které se odkazuji na různé články informující o aktuální situaci na českém trhu, co se hrozeb a napadení firem i jednotlivců v kyberprostoru týče. Odkazují také na důležitost vzdělávání se v této oblasti.

V této práci jsou obsažena a rozebrána všechna témata nezbytná pro dosažení stanoveného cíle práce. Obsah práce by mohl být vodítkem pro podnikatele, kteří chtějí zabezpečení svých webových stránek svěřit do rukou odborníků. Obsahuje data, která by pro ně mohla být užitečná nejen v souvislosti se zabezpečením jejich stránek, ale i ve vztahu k zákazníkům a obavám, které mohou mít například z placení online, což v konečném důsledku může ovlivňovat jejich nákupní chování. Práce v neposlední řadě přináší data a parametry webhostingových firem, které jsou největšími hráči na českém trhu.

4 Seznam použité literatury

4.1 Tištěné zdroje

ANTLOVÁ, K. *Elektronické podnikání.* 1. Liberec: Technická univerzita v Liberci, 2006. 103 s. ISBN 80-7372-086-8.

BASTL, M. *Kybernetický terorismus: studie nekonvenčních forem boje v kontextu soudobého válečnictví*. Brno, 2007. Disertační práce. Masarykova univerzita. Vedoucí práce Prof. PhDr. Maxmilián Strmiska, Ph.D.

BOUČKOVÁ, J. *Základy marketingu*. 4. vyd. Praha: Oeconomica, 2011. ISBN 978-80-245-1760-5

BŘEHOVSKÝ, P. *Sborník příspěvků z XXX. konference EurOpen*. 1. Plzeň: TYPOS Plzeň, 2007, s. 155-161. ISBN 978-80-86583-12-9.

ČERNÁ, A., DĚDKOVÁ, L., MACHÁČKOVÁ, H., ŠEVČÍKOVÁ, A., a ŠMAHEL, D. *Kyberšikana*. 1. Praha: Grada Publishing, 2013. ISBN 978-80-247-4577-0.

FRENDLOVSKÁ, D., JANKOVÁ, M. *Možnosti systémové integrace modelů elektronického podnikání v krizovém kyberprostoru*. Jihlava, 2013. Sborník příspěvků 6. ročníku mezinárodní vědecké konference „Bezpečná Evropa 2013“, 25. 11. 2013. Vysoká škola polytechnická v Jihlavě.

GŘIVNA, T. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. In HORYNA, M. (ed.). *Český právní řád a ochrana kyberprostoru (vybrané problémy)*. Praha: Karolinum, 2008, s. 21-34

GÚČIK, M. *Cestovný ruch pre hotelové a obchodné akadémie.* Bratislava: Slovenské pedagogické nakladateľstvo, 2001. ISBN 80-08-03071-2.

GÚČIK, M. *Cestovný ruch. Úvod do štúdia.* Banská Bystrica: Slovak-Swiss Tourism, 2010, s. 307. ISBN 978-80-89090-80-8.

KOTLER, P. *Moderní marketing: 4. evropské vydání.* Praha: Grada, 2007. ISBN 9788024715452.

KOTLER, P. a G. ARMSTRONG. *Marketing*. Praha: Grada, 2007. ISBN 80-247-0513-3.

LINDEROVÁ, I. *CESTOVNÍ RUCH – Základy a právní úprava*. 1. Vysoká škola polytechnická Jihlava, 2013, s. 10-11. ISBN 978-80-87035-82-5.

LINDEROVÁ, I., SCHOLZ, P., a MUNDUCH, M. *Úvod do metodiky výzkumu*. Jihlava, 2016. Učební text. Vysoká škola polytechnická v Jihlavě.

MACHÁČKOVÁ, H. a T. MIŠKECHOVÁ. *Virtuální zločin: kyberkrádež, kybervražda, kyberznásilnění*. Brno, 2011. Bakalářská práce. Masarykova univerzita. Vedoucí práce PhDr. Pavla Kovářová, Ph.D.

SALACHOVÁ, B. *Právo v podnikání*. 2. Ostrava: KEY Publishing, 2012. ISBN 978-80-7418-148-1.

SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015. s. 636. ISBN 978-80-7380-501-2.

SMEJKAL, V. *Kybernetické nebezpečí a kybernetická válka*. Karlovy Vary, 2013. Sborník příspěvků 6. ročníku mezinárodní vědecké konference „Bezpečná Evropa 2013“, 25. 11. 2013. Vysoká škola Karlovy Vary. s. 142-149.

SUCHÁNEK, P. *Vybrané aspekty elektronického chování.* 2012.

VEBER, J., SRPOVÁ, J., a Kolektiv. *Podnikání malé a střední firmy*. 3. Praha: Grada Publishing, 2012. ISBN 978-80-247-4520-6.

Zákon č. 513/1991 Sb., Obchodní zákoník ve znění pozdějších předpisů.

Zákon č. 127/205 Sb., O elektronických komunikacích a o změně některých souvisejících zákonů (zákon o lektronických komunikacích), ve znění pozdějších předpisů.

4.2 Elektronické zdroje

Sprava-site.eu. *sprava-site.eu* [online]. [cit. 2018-11-29]. Dostupné z: https://www.sprava-site.eu/kyberprostor/

Rpm.fss.muni.cz *Rpm.fss.muni.cz* [online]. [cit. 2018-11-29]. Dostupné z: rpm.fss.muni.cz/Revue/Heslar/kyberprostor.htm

Podnikani-krok-za-krokem.webnode.cz. *Podnikani-krok-za-krokem.webnode.cz*[online]. [cit. 2018-11-29]. Dostupné z: https://podnikani-krok-za-krokem.webnode.cz/definice-podnikani/

Dk.upce.cz. *Dk.upce.cz* [online]. [cit. 2018-11-29]. Dostupné z: https://dk.upce.cz/bitstream/handle/10195/59057/Frendlovsk%C3%A1D_MoznostiSystemove_2014.pdf?sequence=1&isAllowed=y

Goeuro.cz. *Goeuro.cz* [online]. [cit. 2018-11-29]. Dostupné z: https://www.goeuro.cz/autobusy/dopravci/

Czechtourism.cz. *Czechtourism.cz* [online]. [cit. 2018-11-29]. Dostupné z: https://www.czechtourism.cz/

Ttg.cz. *Ttg.cz* [online]. [cit. 2018-11-29]. Dostupné z: http://www.ttg.cz/odbornici-vybrali-nejlepsi-firmy-z-cestovniho-ruchu-v-ceske-republice/

Accka.cz. *Accka.cz* [online]. [cit. 2018-11-29]. Dostupné z: https://www.accka.cz/stranka/zakony-a-dokumenty/seznam-pojistenych-ck/12093

Isic.de. I*sic.de* [online]. [cit. 2018-11-29]. Dostupné z: https://www.isic.de/en/benefits/flixbus/

Tourism.zabreh.cz. *Tourism.zabreh.cz* [online]. [cit. 2018-11-29]. Dostupné z: http://tourism.zabreh.cz/katalog-sluzby-firmy/vlakove-nadrazi/

Designportal.cz. *Designportal.cz* [online]. [cit. 2018-11-29]. Dostupné z: https://www.designportal.cz/leo-express-predstavil-nove-logo-zlatou-strida-oranzova/

Goeuro.cz. *Goeuro.cz* [online]. [cit. 2018-11-29]. Dostupné z: https://www.goeuro.cz/autobusy/dopravci/

Kralvin.cz. *Kralvin.cz* [online]. [cit. 2018-11-29]. Dostupné z: http://www.kralvin.cz/specialni-balicek-praha

Mmr.cz. *Www.mmr.cz* [online]. 2008 [cit. 2019-01-10]. Dostupné z: https://www.mmr.cz/getmedia/a724028c-5ad8-4ea3-ae45-c6fb8440ef19/GetFile13_1.pdf

Ceskapozice.lidovky.cz. *Ceskapozice.lidovky.cz* [online]. [cit. 2019-1-16]. Dostupné z: http://ceskapozice.lidovky.cz/kyberkriminalita-v-cesku-vzrostla-za-sedm-let-temer-ctyrnasobne-phi-/tema.aspx?c=A180515_171751_pozice-tema_lube

Slovacky.denik.cz. *Slovacky.denik.cz* [online]. [cit. 2019-1-16]. Dostupné z: https://slovacky.denik.cz/zlociny-a-soudy/kyberkriminalita-na-slovacku-firmu-chtel-pripravit-o-osm-tisic-euro-20180927.html

Precencekriminality.cz. *Precencekriminality.cz* [online]. [cit. 2019-1-16]. Dostupné z: http://www.prevencekriminality.cz/kyberkriminalita-testovaci-provoz/prevence-kyberkriminality/

Govcert.cz. *Govcert.cz* [online]. [cit. 2019-1-16]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-udalosti/2556-zakladni-kurz-kyberneticke-bezpecnosti-novy-e-learning-k-mesici-kyberneticke-bezpecnosti/

Zprávy.aktualne.cz. *Zprávy.aktualne.cz* [online]. [cit. 2019-1-16]. Dostupné z: https://zpravy.aktualne.cz/ekonomika/kyberneticke-nebezpeci-vzrusta-budte-pripraveni/r~12f13530454011e7a6500025900fea04/

Ostatní seznamy

4.3 Seznam obrázku

4.4 Seznam grafů

4.5 Seznam tabulek

5 Přílohy

5.1 Přílohy A Email

5.1.1 Email v češtině

Dobrý den,
jmenuji se Jana Franková a jsem studentkou cestovního ruchu v Jihlavě. Aktuálně píši bakalářskou práci na téma Kybernetická bezpečnost pro podnikání v kyberprostoru v oblasti cestovního ruchu. Součástí mé práce je výzkumná část, která je zaměřena na zabezpečení webových stránek největších a nejvýznamnějších firem v oblasti cestovního ruchu.
Po telefonické domluvě Vám posílám tento email s prosbou o zodpovězení 2 krátkých otázek.
Zajímá mne, zda si vy, jako firma, zajišťujete sami zabezpečení webových stránek? Nebo se Vám o zabezpečení stará externí firma? Popřípadě jaká?
Děkuji Vám mnohokrát za Váš čas a pomoc.
S pozdravem a přáním příjemného dne,
Jana Franková

5.1.2 Email v angličtině:

Good afternoon,
my name is Jana Franková and I am studying tourism in Jihlava. I am writing my bachelor thesis. Its aim is Cyber-security for business in cyberspace it the field of tourism. Part of this work is research, so I am trying to find out how the biggest companies are solving problems with website security.
I have only 2 short questions. Do you have your onw system how to secure the website or do you have an external firm who cares about this topic? In this case, what is the name of an external company?
Thank you very much for your time and answer which helps me a lot.
Best regards,
Jana Franková

5.2 Příloha B Rozhovor

Dobrý den,
jmenuji se Jana Franková a jsem studentkou cestovního ruchu v Jihlavě. Aktuálně píši bakalářskou práci na téma Kybernetická bezpečnost pro podnikání v kyberprostoru v oblasti cestovního ruchu. Součástí mé práce je výzkumná část, která je zaměřena na zabezpečení webových stránek u firem v oblasti cestovního ruchu. Tyto firmy/společnosti mají většinou externí firmu, která jim zabezpečuje webové stránky. Z tohoto důvodu se obracím na Vás.
Po telefonické domluvě Vám posílám tento email s prosbou o zodpovězení 4 krátkých otázek.
1) Jaké jsou nejčastější hrozby vyskytující se v kyberprostoru a kdo je obvykle provádí?
2) Jakým způsobem řešíte napadení, v případě, že k němu dojde?

3) Dokázal/a byste mi říct, u kterých firem je nejčastější napadení (doprava, ubytování, pojištění, CK, CA)?

4) Jak se vyvarovat případnému napadení?

Děkuji Vám mnohokrát za Váš čas a pomoc.

S pozdravem a přáním příjemného dne,

Jana Franková

5.3 Příloha C Dotazník

Vážená respondentko, vážený respondente,
jmenuji se Jana Franková, jsem studentkou cestovního ruchu na Vysoké škole polytechnické v Jihlavě. Obracím se na Vás s žádostí o vyplnění mého dotazníku, který využiji jako podklad pro mou bakalářskou práci na téma "Kybernetická bezpečnost pro podnikání v kyberprostoru v oblasti cestovního ruchu". Ráda bych poprosila o pravdivé vyplnění dotazníku. Dotazník je anonymní a dobrovolný.
Cílem dotazníkového šetření je zjistit nákupní chování zákazníků, zda platí online, zda jsou seznámeni s riziky placení online a zároveň zda mají nějaké vlastní zkušenosti se zneužitím platebních údajů. Dotazník obsahuje uzavřené, polouzavřené i otevřené otázky. Tento dotazník Vám zabere cca 5 minut. Předem Vám děkuji za spolupráci.

1. Nakupujete na internetu jízdenky/letenky/ubytování/zájezdy/pojištění?
   - Ano
   - Ne (pokud jste vybral/a tuto odpověď, přejděte prosím na otázku č. 10)
2. Platíte za nákup výše zmíněných produktů online?
   - Ano
   - Ne
3. Jakým způsobem platíte nejčastěji v případě nákupu online?
   - Platba kartou online
   - Bankovním převodem
   - Preferuji platit na místě, pokud možno
   - Jiná ……..
4. Za jakou službu z následujících nejčastěji platíte online?
   - Doprava
   - Ubytování
   - Nákup zájezdů
   - Pojištění
   - Jiná ……
5. O jakých hrozbách při platbě online víte?
   - Hacker
   - Cracker
   - Phishing
   - Pharming
   - Sniffing
   - Jiná ……

Hacker - "záškodník", který se snaží dostat někam, kam nemá a narušit cizí počítačový systém.

Cracker – označení člověka s výbornými znalosti v oblasti počítačů, který se nabourává do cizích sítí a systémů za účelem uškodit.

Phishing – útočník rozesílá mail, v něm se vydává za banku a požaduje buď sdělení určitých údajů, nebo provedení nějaké operace (např. kliknutí na přiložený odkaz). Cílem podvodných emailů je získání přihlašovacích údajů k internetovému bankovnictví. Pharming – útočník využívá speciální počítačové programy, které

uživatele při přihlášení do internetového bankovnictví přesměrují na stránky, jež vypadají jako originální stránky, ale ve skutečnosti jsou pouze jejich napodobeninou.
Sniffing – technika umožňující odposlouchávání počítačů v lokální síti, která se používá např. při diagnostice sítě. Sniffing nahrazuje činnost spywaru (špionáž dat) či keyloggeru (zjištění hesel).

6. Máte nějaké obavy při platbě online (platba kartou online, bankovní převod)?
    - Ano
    - Ne
7. Pokud ano, čeho se nejvíce obáváte?
    - ……
8. Máte Vy osobně nějakou zkušenost se zneužitím platebních či jiných údajů?
    - Ano
    - Ne
9. Pokud jste odpověděl/a ano, o jakou zkušenost se jedná?
    - ……
10. Uveďte prosím Vaše pohlaví.
    - Žena
    - Muž
11. Uveďte prosím Váš věk.
    - Do 18
    - 19 – 25
    - 26 – 35
    - 36 – 45
    - 46 – 55
    - 56 a více let
12. Jaké je Vaše nejvyšší dosažené vzdělání?
    - Střední odborné učiliště bez maturity
    - Střední odborné učiliště s maturitou
    - Střední škola s maturitou
    - Vyšší odborná škola
    - Vysoká škola (titul Bc.)
    - Vysoká škola (titul Mgr., Ing., MUDr., JUDr.)

13. Uveďte prosím místo Vašeho bydliště.

- Méně jak 2 000 obyvatel
- 2 001 – 5 000 obyvatel
- 5 001 – 10 000 obyvatel
- 10 001 – 20 000 obyvatel
- 20 001 – 50 000 obyvatel
- 50 001 – 100 000 obyvatel
- 100 001 – 200 000 obyvatel
- 200 001 – 500 000 obyvatel
- Nad 500 001 obyvatel

14. Z jakého kraje pocházíte?

- Hlavní město Praha
- Středočeský kraj
- Jihočeský kraj
- Plzeňský kraj
- Karlovarský kraj
- Ústecký kraj
- Liberecký kraj
- Královéhradecký kraj
- Pardubický kraj
- Kraj Vysočina
- Jihomoravský kraj
- Olomoucký kraj
- Zlínský kraj
- Moravskoslezský kraj