Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Bezpečnost sociálních sítí

Aleš Caisek

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Aleš Caisek

Informatika

Název práce

Bezpečnost sociálních sítí

Název anglicky

Safety of Social Network Sites

Cíle práce

Cílem práce je analyzovat možné způsoby současného zneužívání sociálních sítí, porovnáním bezpečnostních skandálů identifikovat nejčastější příčiny bezpečnostních hrozeb a navrhnout způsoby snížení jejich rizika.

Dílčím cílem práce bude vyvrátit či potvrdit předpoklad nízkého stupně zabezpečení přihlašovacích údajů uživatelských účtů na sociálních sítích.

Metodika

Hlavními opěrnými body teoretické části práce bude studium odborné literatury

podrobně popisující sociální média, jejich charakteristiky a souvislosti, bezpečnost a rizika. Hlavním zdrojem budou především vědecké a odborné články a knihy.

Praktická část bude zaměřena na zjištění současného stupně zabezpečení přihlašovacích údajů uživatelů na sociálních sítích. Provedena bude metodou dotazníkového šetření s následným vyhodnocením. Dotazníkové šetření bude zahrnovat typické cílové skupiny příslušných sociálních sítí podle předem analyzované demografie.

Doporučený rozsah práce

30 – 40 stran

Klíčová slova

sociální sítě, bezpečnost, rizika, bezpečnostní hrozby, uživatelské účty, facebook, twitter

---

Doporučené zdroje informací

ALTSHULER, Yaniv. Security and privacy in social networks. New York: Springer, c2013, vi, 253 p. ISBN 1461441382.

ANDREWS, Lori. I know who you are and I saw what you did: social networks and the death of privacy. 1st Free Press trade pbk. ed. New York: Free Press, 2013. ISBN 9781451651058.

CROSS, Michael. Social media security: leveraging social networking while mitigating risk. xvii, 328 pages. ISBN 9781597499866.

CHBEIR, Richard a Bechara Al BOUNA. Security and privacy preserving in social networks. New York: Springer, 2013, xvi, 367 pages. Lecture notes in social networks. ISBN 9783709108949.

RYAN, Peter K. Social networking. 1st ed. New York: Rosen Central, 2010, p. cm. ISBN 97814488230176.

Předběžný termín obhajoby

2018/19 LS – PEF

Vedoucí práce

Ing. Václav Lohr, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 28. 10. 2015

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 10. 11. 2015

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 09. 11. 2018

Čestné prohlášení

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

V Praze dne _____

Poděkování

Rád bych touto cestou poděkoval Ing. Václavu Lohrovi Ph.D. za jeho rady a připomínky při vypracování mé bakalářské práce.

Bezpečnost sociálních sítí

Souhrn

Tato práce se zaměřuje na možné způsoby současného zneužívání sociálních sítí a navrhuje snížení jejich rizika. V teoretické části pojednává o sociálních sítích, definuje tento pojem, uvádí jejich charakteristiky a představuje nejdůležitější sociální sítě. Druhá podkapitola se zaměřuje na bezpečnost sociálních sítí a rizika spojená se sociálními sítěmi, čímž pojednává jednak o pravidlech bezpečného chování na sociálních sítích (s důrazem na zabezpečení uživatelského účtu), ale zaměřuje se i na nejvýznamnější rizika a hrozby, které se v současné době se sociálními sítěmi pojí.

Praktická část práce pak sestává z kapitoly nazvané vlastní práce, která je zaměřena především na zjištění současného stupně zabezpečení přihlašovacích údajů uživatelů na sociálních sítích prostřednictvím dotazníkového šetření.

Klíčová slova: sociální sítě, bezpečnost, rizika, bezpečnostní hrozby, uživatelské účty

Safety of Social Network Sites

Abstract

This thesis focuses on possible ways of abusing of social networks and proposes reducing their risks. In the theoretical part it deals with social networks, defines this concept, presents their characteristics and represents the most important social networks. The second subchapter focuses on social network security and social networking risks, which deals with rules on safe social behavior (focusing on security of the user account), but also focuses on the most important risks and threats that currently occur social networks.

The practical part of the thesis consists of a chapter called own work, which is mainly focused on finding out the current level of security of users login on social networks through a questionnaire survey.

Keywords: social networks, security, risks, security threats, user accounts

Obsah

Seznam grafů

1 Úvod

Tématem předkládané studie je bezpečnost sociálních sítí. Téma lze považovat z velmi aktuální, neboť většina příslušníků mladších generací v současné době používá některou ze sociálních sítí, je poměrně obvyklé, že lidé mají profily na více různých sociálních sítích. Na jednu stranu je pravdou, že sociální sítě mají řadu výhod, umožňují snazší kontakt mezi lidmi prostřednictvím messengerů stejně jako možnost sdílet s okolím své zážitky a postoje i několikrát za den, a to navzdory skutečnosti, že v realitě zdaleka tolik času na vzájemný kontakt není. Výhodou může být i komunikace na dálku (klidně na druhý konec světa, která je přitom takřka zdarma, postačuje, aby byl člověk připojen k internetu). Sociální sítě umožňují rovněž obnovit kontakt například s dávnými známými nebo třeba s bývalými spolužáky, které člověk dlouho neviděl. V současné době jsou sociální sítě často i významným zdrojem informací stejně jako je leckdy možné přes ně realizovat i nákup nebo prodej zboží či služeb. Řada uživatelů tak při každodenním využívání pozitiv, která sociální sítě nabízejí, zapomíná na bezpečnost a dostatečné zabezpečení svých profilů na sociální síti.

Realita je však taková, že vedle řady pozitiv s sebou sociální sítě nesou i celou řadu bezpečnostních rizik. K jejich nejběžnějším případům tak patří například kyberšikana, kyberstalking, navázání kontaktu s rizikovým jedincem (osobou, která se např. snaží získat osobní informace za účelem jejich zneužití nebo třeba páchání trestné činnosti), počítačové viry, zneužití osobních údajů nebo dokonce krádež identity, které bývají typicky spojeny zejména s nedostatečným zabezpečením profilu na sociální síti

Následující text je standardně členěn na dvě části, a to na část teoretickou a část analytickou. Toto členění pak sestává celkem ze šesti kapitol. První kapitolu tvoří tento úvod, druhá kapitola představuje cíle práce a metodiku zpracování výzkumu, třetí kapitola je věnována teoretickým východiskům a sestává ze dvou podkapitol, kdy první podkapitola pojednává o sociálních sítích, definuje tento pojem, uvádí jejich charakteristiky a představuje nejdůležitější sociální sítě, zatímco druhá podkapitola se zaměřuje na bezpečnost sociálních sítí a rizika spojená se sociálními sítěmi, čímž pojednává jednak o pravidlech bezpečného chování na sociálních sítích (s důrazem na zabezpečení uživatelského účtu), ale zaměřuje se i na nejvýznamnější rizika a hrozby, které se v současné době se sociálními sítěmi pojí.

Praktická část práce pak sestává z kapitoly nazvané vlastní práce, která je zaměřena především na zjištění současného stupně zabezpečení přihlašovacích údajů uživatelů na sociálních sítích prostřednictvím dotazníkového šetření. V této kapitole je tedy vyhodnoceno dotazníkové šetření a navazující pátou kapitolu pak tvoří výsledky dotazníkového šetření a zhodnocení stanovených cílů a konečně jsou zde také formulována doporučení pro praxi. Poslední kapitolu práce pak tvoří závěr, který stručně shrnuje nejpodstatnější zjištění.

2 CÍL PRÁCE A METODIKA

Na počátku každé vědecké práce je nutné si stanovit cíle, které mají být naplněny a v návaznosti na ně formulovat metodický postup, jehož prostřednictvím má být cílů dosaženo. Právě tyto dvě nezbytné složky práce představuje tato kapitola.

2.1 Cíl práce

Cílem práce je analyzovat možné způsoby současného zneužívání sociálních sítí, porovnáním bezpečnostních skandálů identifikovat nejčastější příčiny bezpečnostních hrozeb a navrhnout způsoby snížení jejich rizika. Dílčím cílem práce je vyvrátit či potvrdit předpoklad nízkého stupně zabezpečení přihlašovacích údajů uživatelských účtů na sociálních sítích.

2.2 Metodika

Vlastní metodický postup práce započal již tím, že došlo k prostudování odborné literatury, stanovení cílů, kterých má být dosaženo a následné volbě metody, jejímž prostřednictvím má být cílů dosaženo. Zvolena byla kvantitativní výzkumná strategie, jejíž výhodou je především skutečnost, že je možné výsledky kvantifikovat, statisticky ověřit a zobecnit buď na celou populaci nebo na určitou část populace (tj. umožňuje formulovat šířeji platná zjištění), která je předmětem zkoumání. Nevýhodou kvantitativního výzkumu však může být fakt, že jeho prostřednictvím není vždy možné jít dostatečně do hloubky zkoumaného problému, nemusí se tak podařit vysledovat veškeré příčiny a souvislosti. Výzkumník se prostřednictvím kvantitativního výzkumu snaží postihnout spíše obecnější zákonitosti zkoumané problematiky (Sedláková, 2014, s. 52). Pro účely výzkumu realizovaného v této práci byl tak kvantitativní výzkum vhodnější než výzkum kvalitativní.

Konkrétní technikou, která byla zvolena za účelem realizace výzkumu, je pak dotazníkové šetření. Dotazník je velmi osvědčenou a zároveň oblíbenou metodou sběru dat, neboť se vyznačuje především nízkou finanční, ale také časovou náročností, což je z pozice

výzkumníka velmi vítáno. Z pohledu respondenta je pak velkým pozitivem, že dotazník obvykle zajišťuje poměrně velkou míru anonymity (Havlíčková, 2015, s. 31).

V rámci předkládaného výzkumu je využit nestandardizovaný polostrukturovaný dotazník, jehož úplné znění je přiloženo v příloze č. 1 této práce. Dotazník sestává celkem z 20 otázek, z nichž část je zaměřena na charakteristiku výzkumného souboru, část je zaměřena obecně na využívání sociálních sítí a část je zaměřena konkrétně na otázku zabezpečení přihlašovacích údajů uživatelů sociálních sítí a obecně na otázky bezpečnosti na sociálních sítích. Otázky, které tvoří dotazník jsou koncipovány jako uzavřené, což znamená, že respondent jednoduše volí jednu z nabízených možností, která nejlépe odpovídá jeho situaci, popř. jeho postoji k otázce. Uzavřená otázka by měla obsahovat alternativy, které pokrývají všechny možné odpovědi (Disman, 2011, s. 127).

Vedle uzavřených otázek je pak dotazník v některých případech doplněn o otázky polootevřené, které vedle několika možných alternativ odpovědí nabízejí i možnost zvolit variantu „jiné," a následně vlastními slovy dopsat respondentovu odpověď, která není alternativami pokryta.

Poté co byla sestavena první verze dotazníku, byla nejprve provedena pilotní studie Na rozdíl od vlastního šetření byla v případě pilotní studie zvolena kvalitativní výzkumná strategie, která mohla lépe napomoci prověřit otázky v dotazníku jak po stránce obsahové, tak po stránce formální a odhalit nejasnosti, nepřesnosti či nesprávné formulace v dotazníku, které by mohly vést k nesprávnému pochopení dotazu, případně být vykládány dvojznačně. Pilotní studie se však zaměřovala i na opravu případných gramatických chyb stejně jako stylistických nedostatků, aby bylo zajištěno, že dotazník bude ze strany respondentů přijat co nejlépe a poskytne relevantní informace, ze kterých bude možné vyvodit adekvátní výsledky. Pilotní studie byla realizována s celkem pěti respondenty ve věku 20-35 let (vlastní výzkum pak v kontextu vyšší variability zahrnoval respondenty ve věku 18-35 let), kteří jsou pravidelnými uživateli sociálních sítí. Respondenti pro pilotní studii byli vybíráni na základě rodinných a profesních kontaktů výzkumníka. S každým respondentem v rámci pilotní studie byl celý dotazník projit,

respondent jej společně s výzkumníkem měl pokusit vyplnit, ale zároveň byl formou nestandardizovaného rozhovoru (Disman, 2011, s. 121) dotazován na srozumitelnost otázek, zda považuje odpovědi za relevantní, zda mu nějaká odpověď mezi nabízenými chybí, popř. zdaje podle něj některá otázka dvojznačná apod. Z nestandardizovaných rozhovorů nad dotazníky byly pořizovány poznámky, které byly vpisovány přímo k rozhovorům. Následně byly poznámky vyhodnoceny a v návaznosti na některé z nich, které se buď opakovaly, případně se ukázaly být pro výzkum podnětné, byly dotazníky poupraveny. Úpravy byly realizovány zejména po stylistické stránce, kdy docházelo k přeformulování některých dotazů, v ojedinělých případech vedla pilotní studie rovněž k doplnění variant odpovědí v dotazníku. Tímto postupem tak vznikla finální verze dotazníku, jejímž prostřednictvím pak byla sbírána data pro účely vlastního výzkumu.

Vlastní sběr dat probíhal za pomocí internetového online systému Survio, do kterého byla finální verze dotazníku zadána a následně byl dotazník distribuován prostřednictvím internetového odkazu. S ohledem na skutečnost, že se dotazník zaměřoval na sociální sítě, byl distribuován jednak na sociálních sítích, dále byl distribuován prostřednictvím internetových diskusí a prostřednictvím e-mailu na kontakty, které měl k dispozici výzkumník. Vlastní sběr dat probíhal v měsíci červenci 2018, a to po dobu 14 dnů, následně byl dotazník ukončen a bylo přistoupeno k jeho vyhodnocení. Celkem dotazník vyplnilo 126 osob, které dotazníky také dokončili a vyplnili správně, tj. nebylo nutné žádný dotazník vyřadit.

Vyhodnocení dotazníkového šetření probíhalo za pomocí programu MS Excel, ve kterém bylo realizováno statistické zpracování včetně zjištění absolutních a relativních četností jednotlivých odpovědí, v MS Excel byly také vytvořeny grafy a tabulky, které jsou součástí analytické části této práce. Statistická data byla následně doplněna slovními komentáři. Za pomocí metody syntézy a dedukce pak byly dávány do souvislosti odpovědi na nejrůznější otázky v dotazníků a byly také vyhodnoceny stanovené cíle. Prostřednictvím dedukce pak byly formulovány rovněž závěry a doporučení pro praxi. V rámci diskuse je pak využita rovněž metoda komparace, neboť zde dochází ke srovnání výsledků realizovaného výzkumu s dalšími výzkumy jiných autorů, kteří se podobně zaměřeným výzkumům věnovali dříve.

3 TEORETICKÁ VÝCHODISKA

Kapitola zaměřená na teoretická východiska obsahuje především východiska týkající se sociálních sítí a východiska týkající se bezpečnosti a bezpečnostních rizik na sociálních sítí (včetně zabezpečení uživatelských účtů).

3.1 Sociální sítě

Sociální sítě jsou fenoménem současné doby, téměř každý člověk o nich alespoň slyšel a poměrně velká část populace s nimi má vlastní zkušenost. Přesto je však nutné v této práci pojem sociální síť nejprve vymezit a následně charakterizovat, aby bylo zajištěno, že bude čtenář vnímat pojem sociální síť stejným, popř. alespoň velmi podobným způsobem jako autor tohoto textu. Aby bylo možné o sociálních sítích pojednat v konkrétnější rovině, jsou pak představeny rovněž nejznámější sociální sítě současné doby.

3.1.1 Definice sociální sítě

Již ze samotného pojmu „sociální“ lze mít za to, že sociální síť má jednoznačně souvislost se společností. Takřka každý člověk si pod pojmem sociální síť dokáže něco představit, laické představy o tom, co se rozumí sociální sítí však nemusí být a obvykle ani nebývají příliš přesné. Proto je žádoucí přistoupit k vymezení tohoto pojmu na základě studia odborné literatury.

V odborné literatuře je možné najít vícero různých definic pojmu sociální síť. Lze se setkat například s tvrzením, že *„Sociální síť, zvaná též společenská síť, komunitní síť či komunita, anglicky social network, je propojená skupina lidí. V širším slova smyslu je sociální sítí každá skupina lidí, která spolu udržuje komunikaci různými prostředky. V užším, moderním a značně převažujícím pojetí se sociální sítí nazývá služba na internetu, která registrovaným členům umožňuje si vytvářet osobní (či firemní) veřejný či částečně veřejný profil, komunikovat spolu, sdílet informace, fotografie, videa, provozovat „chat“ a další aktivity.“(*Burian, 2014, s. 84). V návaznosti na uvedenou definici je pak třeba upřesnit, že v dalším textu této práce, se pod pojmem sociální síť rozumí právě sociální síť v užším smyslu slova.

Výše uvedená definice však není zdaleka jediná. Poněkud techničtěji orientované vymezení pak říká, že pod pojmem sociální sítě lze rozumět novou generaci internetových služeb, kde obsah vytvářejí přímo její uživatelé (Ting, 2010, s. 92). Lze rovněž říct, že se jedná vlastně o specializované webhostingové služby v kombinaci se specializovaným vyhledávačem (Procházka, 2010, s. 57).

Ačkoliv se všechny tři uvedené definice sociální sítě navzájem poměrně významně liší, lze identifikovat některé aspekty, které mají společné. Jedná se vlastně o určitou webovou stránku, na které se vazby mezi jejími uživateli, vytvářejí v návaznosti na určitou sociální strukturu. Sociální síť tak sdružuje jedince, kteří mají nějaké společné zájmy, spojuje je společné přátelství nebo třeba profese.

3.1.2 Charakteristika sociálních sítí

Základním charakteristickým rysem sociálních sítí je především možnost uživatele vytvořit si vlastní profil na sociální síti. Dalším charakteristickým rysem sociálních sítí je skutečnost, že umožňují vzájemnou socializaci, tedy nalézání přátel se stejnými zájmy nebo třeba se stejnou profesí stejně jako umožňují velmi snadnou a rychlou komunikaci jejich uživatelů. Sociální sítě totiž především spoléhají na to, že si jejich uživatelé budují vlastní síť kontaktů, čímž mimo jiné získávají přístup k dalším kontaktům, vznikají tak doporučení na další kontakty, což napomáhá růstu a rozvoji sociální sítě. Komunikace mezi uživateli (jak v rámci vlastí sítě, tak i mimo ni) je obvykle možná buď prostřednictvím vzkazů (interní pošty, chatu, instant messengerů) nebo i formou otevřené komunikace (tzv. na zdi)(Peacock, 2012, s. 18).

Sociální sítě jsou novým způsobem, jak probíhá komunikace mezi lidmi, ale i způsobem utváření sociálních vazeb mezi jednotlivými uživateli sociálních sítí. Sociální sítě však vytvářejí i nové prostory, kde spolu lidé komunikují (např. skupiny, stránky na sociálních sítích) stejně jako přináší celou řadu nových nástrojů mezilidské komunikace (Pospíšilová, 2016, s. 18). Sociální sítě lze dále charakterizovat jako prostor, ve kterém je možné velmi efektivně jak navazovat, tak realizovat spolupráci na společném projektu, zakázce či čemkoli, na čem se uživatelé dohodnou. Sociální sítě totiž existují především proto, že je jejich uživatelé plní svým obsahem. Bez obsahu od uživatelů by sociální síť neměla význam. Jsou to pak právě uživatelé, kdo tvoří obsah a dávají smysl fungování sociální sítě (nezávisle na tom, zda ji využívají jako volnočasovou aktivitu, za účelem spolupráce nebo třeba za účelem marketingu)(Bednář, 2011, s. 193).

Specifickým rysem sociálních sítí je pak zejména fakt, že dávají uživateli možnost být v kontaktu s velkým počtem osob, se kterým by leckdy přímý kontakt nebyl reálný buď z důvodu jejich počtu, ale také třeba z důvodu jejich geografické vzdálenosti, sociální síť totiž velmi snadno umožňuje udržovat kontakt i s lidmi na druhém konci světa. Sociální sítě umožňují také velmi jednoduché, a navíc flexibilní sdílení informací (ale i materiálů, dokumentů, fotografií či videí) mezi uživateli, dává uživatelům možnost se vzájemně vyhledávat. Důležitým charakteristickým rysem je také skutečnost, že sociální sítě umožňují sdílení informací, ale i zprostředkování kontaktu zcela nezávisle na denní či noční hodině, tj. zcela kdykoliv, kdy o to mají uživatelé zájem.

Velký význam má rovněž využití sociálních sítí jako marketingového či komunikačního nástroje ze strany firem, ale třeba i ze strany neziskových organizací. Sociální sítě jsou tak leckdy zdrojem návštěvníků pro web organizace, ale i nástrojem, který společnosti přivádí četné zákazníky. Na řadě sociálních sítí lze dnes také inzerovat zboží či služby či je přímo poskytovat (prodávat zboží). To vše má z hlediska marketingu zásadní význam i proto, že sociální sítě často umožňují přístup ke specifickým segmentům veřejnosti, čímž podniky, jejichž cílová skupina se nachází mezi uživateli sociálních sítí, mají dobrý důvod zde své produkty či služby propagovat (Svoboda, 2009, s. 171).

Při charakteristice sociálních sítí nelze opomenout ani skutečnost, že sociální sítě postupem času začínají tvořit významnou část internetového obsahu. Je možné zde dohledat skutečně nespočet informací, nalézt zde své staré známé, ale i nové přátele stejně jako dávají prostor pro diskusi, leckdy poskytují prostor pro získání informací a vznášení dotazů, na které je možné reagovat. Sociální síť také umožňuje tvořit vlastní příspěvky (na vlastním profilu, na blogu apod (Procházka, 2010, s. 57).

Z hlediska účelu, který sociální sítě plní, lze identifikovat dva základní účely. Prvním je udržování kontaktu mezi jednotlivými uživateli sociální sítě a související budování sítě kontaktů, se kterým je pak možné vytvářet i spolupracující komunitu. Druhým účelem sociálních sítí je pak šíření informací, které provádějí samotní uživatelé právě prostřednictvím vytvořené sítě kontaktů a spolupracujících komunit (Peacock, 2012, s. 18).

3.1.3 Nejznámější sociální sítě

K nejznámějším sociálním sítím dnešní doby patří zcela jistě Facebook, Twitter, LinkedIn, Instagram stejně jako třeba Google+. Vedle toho existuje i řada dalších sociálních sítí, nicméně v následujícím textu jsou představeny pouze výše uvedené, neboť není cílem práce poskytnout popis existujících sociálních sítí, mělo by však být stručně pojednáno o tom, k čemu jsou jednotlivé nejčastěji používané sítě dobré, jaké mají funkce a co vše svým uživatelům nabízejí a umožňují.

Facebook je jednou z vůbec nejznámějších a nejoblíbenějších sociálních sítí současnosti. Jedná se o sociální síť, která vznikla v roce 2004, jejími zakladateli byli studenti Harwardské university jako Mark Zuckerberger, Eduard Saverin a další. Prvotní myšlenkou Facebooku bylo sdílení informací, fotografií a materiálů právě mezi studenty, kteří byli zároveň přáteli – studenty Harwardské univerzity (Burian, 2014, s. 84). Facebook sám o sobě je vlastně jen určitou platformou, jejímž prostřednictvím je možné sdílet celou řadu informací a dat stejně jako komunikovat. V oblasti komunikaci dnes Facebook ve své podstatě konkuruje telefonům či e-mailům, přes Facebok se dají posílat vzkazy i telefonovat, dokonce je možné použít i videohovory (Dědiček, 2016, s. 7).

Podstata sdílení informací či komunikace přes Facebook spočívá na navazování „přátelství," neboť příspěvky je možné sdílet buď pouze s osobami, které má jedinec v přátelích nebo s veřejností, případně je možné přátele různým způsobem kategorizovat a strukturovat a sdílet tak některé příspěvky např. jen s určitou skupinou přátel (například dle zájmů, profese apod.). Navazování přátelství na Facebooku je přitom charakteristické svojí reciprocitou, tj. přátelství musí potvrdit obě strany, jinak není možné sledovat příspěvky toho druhého určené pouze přátelům. Neopomenutelnou složkou Facebooku jsou pak stránky, které je možné sledovat a označovat *„To se mi líbí,"* čímž je možné vyjádřit sympatie např. určité značce kosmetiky, vína či nějaké organizaci či spolku dle preferencí uživatele. Stejně tak je možné se účastnit skupin, do kterých je možné se přidat a sdílet zde informace vztahující se k tématu skupiny (opět může jít o zájmy, profesi, znalosti apod.). Vedle toho nabízí velmi silný nástroj, kterým jsou události, jehož prostřednictvím lze uspořádat a upozornit uživatele Facebooku na určitou společenskou či kulturní akci (může se jednat jak o soukromou oslavu, která je určena např. jen přátelům určitého uživatele, ale i o veřejnou akci, o které se takto uživatelé nejen dozvědí,

ale jsou pak Facebookem upozorňováni na to, že ji mají naplánovanou, pokud projeví zájem se jí účastnit). Specifickým rysem Facebooku je skutečnost, že sám o sobě je Facebook pouze platformou určenou ke komunikaci a sdílení, a je to právě jeho obsah, který vytvářejí přímo jeho uživatelé, který jej činí bohatým zdrojem informací. Facebook je v současné době stále se rozvíjející službou, která rozšiřuje nabídku svých služeb a dává tak uživatelům čím dál tím více možností, jak jej využívat (Dědiček, 2016, s. 7).

Twitter je vlastně *„služba sociální sítě (pro komunikaci mezi lidmi prostřednictvím webových stránek), umožňující uživatelům příspěvky posílat a číst příspěvky zaslané jinými uživateli, známé jako tweety. Tweet je textový příspěvek dlouhý maximálně 140 znaků který se zobrazuje na uživatelově profilové stránce a na stránkách těch, kteří ho sledují („followers*“).“(Král, 2016, s. 153).

Twitter nabízí možnost omezit uživatelovy příspěvky jen na některé uživatele, ale také ponechat příspěvky dostupné komukoliv (takto je koncipováno výchozí nastavení). Na Twitteru lidé mohou sledovat osobu, kterou znají, ale třeba i osobu, která je jim sympatická stejně jako známkou osobnost, přičemž pro sledování zde není požadována reciprocita. Je tudíž možné, aby jedinec A sledoval jedince B, ale jedinec B nemusí přitom sledovat jedince A. Twitter byl založen v roce 2006 Jackem Dorseyem, jedná se o velmi oblíbenou sociální síť, nicméně ve srovnání s Facebookem nabízí jen velmi omezené služby, naopak její výhodou je velmi dobrá funkčnost, a to jak na počítači, tak v mobilu i přes různé aplikace v mobilech či tabletech (Král, 2016, s. 153). Podstata Twitteru spočívá tedy s ohledem na možnost publikovat pouze krátké komentáře v tzv. mikroblogingu. Podstata blogování (blogingu) spočívá v tom, že uživatel prezentuje své vlastní názory, zkušenosti a prožitky, vyjadřuje se k aktuálním tématům. Mikrobloging je pak specifickou formou blogingu, která se vyznačuje především krátkým rozsahem příspěvků, které jsou ovšem i tak často velmi výstižné a vyjadřují vlastní myšlenku, reprezentují citáty nebo parafráze, ale i glosy či reflexe (Burian, 2014, s. 84).

LinkedIn je sociální síť, která je na rozdíl od výše uvedených dvou, zamřená především na oblast businessu, spojuje tedy primárně obchodní partnery, kolegy z práce či spolužáky ze škol. Základní myšlenka je zaměřena právě na zprostředkování kontaktů obchodních partnerů, ale i na vyhledávání nových obchodních partnerů stejně jako na vyhledávání zaměstnanců (popř. i zaměstnavatelů), které může uživatel oslovit. LinkedIn bývá obvykle primárně plněn

informacemi o vzdělání, profesních zkušenostech, dovednostech, schopnostech, znalostech a profesním zaměření jednotlivce, popř. informacemi o zaměření a fungování firmy. Důležitou funkcí, kterou LinkedIn rovněž nabízí je doporučování uživatelů, popř. potvrzování dovedností, které uživatel na svém profilu uvádí. To může být velmi důležité například při hledání nového zaměstnání, kde může reference či potvrzení dovednosti mít pozitivní dopad na výběr vhodných kandidátů, popř. I na vlastní výběrové řízení na pozici. LinkedIn dále umožňuje také vývojářům vytváření dalších aplikací a lze jej propojit například s Twitterem (Peacock, 2012, s. 20-21).

Instagram je sociální sítí, která je zaměřena primárně umělecky, její základní podstata spočívá v tom, že jsou zde sdíleny fotografie a videa, přičemž fotografie lze na síti také upravovat prostřednictvím celé řady různých filtrů (Herodek, 2014, s. 201). Uživatelé zde mají své profily a další uživatelé se mohou stát fanouškem takového profilu, čímž je možné mezi uživateli udržovat určitý kontakt (zejména mají uživatelé možnost fotografie a videa hodnotit, a to i prostřednictvím emotikon, reagovat na ně apod.). Specifickým rysem je rovněž skutečnost, že Instagram je primárně mobilovou aplikací, jejímž prostřednictvím lze fotografie a videa, která byla telefonem pořízena primárně sdílet, přes počítač se lze sice k profilu rovněž dostat, nicméně využití není zdaleka tak frekventované a efektivní jako v případě mobilní aplikace. Vedle udržování kontaktu s nespočtem lidí prostřednictvím sdílení fotografií a videí má Instragram v současné době rovněž marketingové využití. Instagram byl založen v roce 2009, a to dvěma zakladateli – Mikem Kriegerem a Kevinem Systromem (Mattern, 2017, s. 5-7).

Google + je sociální síť, která vznikla v roce 2011 jako jedna ze služeb světového internetového vyhledávače Google. Na počátku bylo možné se k sociální síti Google + připojit pouze na základě pozvánky, což byl velmi vhodný marketingový tah, neboť o tyto pozvánky byl velký zájem. Google + přinesl novinku, kterou byly tzv. kruhy za účelem seskupování kontaktů (dnes je možné vytvářet skupiny kontaktů i na jiných sítích, například na Facebooku, nicméně seskupování funguje na trochu jiném principu). Google + nabízí například kruhy rodina, práce, škola apod. V případě sdílení jakékoliv informace tak bylo možné vybrat si, se kterým kruhem bude informace sdílena, což umožňuje větší systematizaci (například informace určené kolegům z práce se zobrazí jen jim, informace určené pro rodinu se zase zobrazí jen rodinným příslušníkům, čímž uživatelé nejsou zatěžováni informacemi, které pro ně nejsou podstatné či přínosné). Na druhou stranu kruhy není nutné používat.

Podobně jako Facebook umožňuje Google+ sdílet například fotografie, textová sdělení, videa apod. dává navíc prostor reflektovat na informace například tlačítkem +1, kterým může dát jeden uživatel jinému najevo, že se mu jeho příspěvek líbí, hodnotí ho pozitivně. Google + také umožnil prostřednictvím aplikace Hangouts například konferenční hovory v jednotlivých skupinách, disponuje rovněž řadou nástrojů pro úpravu fotografií. Nicméně ačkoliv byl na počátku o Google + velký zájem, v současné době se jedná o síť sice známou, nicméně běžnými uživateli ne příliš využívanou. Užitečná může být spíše pro firmy, které tak mají možnost sdílet potřebné informace například se zaměstnanci, které lze rozdělit do jednotlivých kruhů podle toho, v jakém oddělení firmy pracují. Stejně tak je prý poměrně výrazně využíván specifickými komunitami uživatelů, a to například komunitami lidí, kteří nemají zájem sledovat marketingové nástroje, komerční profily a reklamy, jichž je v současné době plný třeba Facebook. Naopak z hlediska marketingu je Google + v současné době prakticky nevyužitelný (1).

3.2 Bezpečnost sociálních sítí a bezpečnostní rizika

Vedle samotného pojednání o sociálních sítích je součástí teoretických východisek práce rovněž pojednání o bezpečnosti na sociálních sítích, kde je nejprve definován pojem bezpečnostní riziko, dále jsou uvedena základní pravidla a doporučení bezpečného chování na sociálních sítích. Dále je samostatná podkapitola zaměřena na zabezpečení účtu na sociálních sítích, které je hlavní oblastí výzkumu v této práci a pro účely komplexního pojednání o bezpečnosti a bezpečnostních rizicích na sociálních sítích jsou zmíněny i vybrané hrozby.

3.2.1 Pojem bezpečnostní riziko

Samotný pojem riziko pochází již ze 17. století, má tedy poměrně dlouhou tradici a nejedná se rozhodně o nový termín. Tehdy byl však spojován primárně s lodní platbou, dnes se jedná o výraz, který se používá poměrně univerzálně, internet a sociální sítě nevyjímaje. Lze jej chápat vlastně jako určitá úskalí, která je třeba eliminovat. Později se však pod pojmem riziko rozumělo spíše vystavení nepříznivým okolnostem. V dnešním pojetí je riziko nejspíše vnímáno jako nebezpečí vzniku nějaké ztráty či škody, případně nebezpečí nějakého poškození či nezdaru. Lze jej vnímat také jako *„podmínku reálného světa, v němž existuje vystavení nepříznivým okolnostem“*(Smejkal, Karel, 2013, s. 90-91).

Pokud se jedná o riziko bezpečnostní, je pak nutné vykládat tento pojem pouze v kontextu bezpečnosti (pro účely této práce pro účely bezpečnosti na sociálních sítích), nikoliv v kontextu obecném. Bezpečnostní riziko je tedy riziko, které je spojeno s bezpečností osob (především jejich života a zdraví), popř. i jejich majetku stejně jako s bezpečností informací(2), což je právě na sociálních sítích velmi důležité.

3.2.2 Základní pravidla bezpečného chování na sociálních sítích

V souvislosti s užíváním sociálních sítí se lze setkat s celou řadou doporučení či zásad, jak se vyvarovat bezpečnostním rizikům s užíváním sociálních sítí spojených. Předně je nutné vždy počítat s tím, že jakákoliv aktivita na sociálních sítích (sdílení informací, fotek, komentování příspěvků apod.) může být v budoucnu nějakým způsobem zneužita třetí stranou. Je tedy vždy třeba zvážit, zda určitou aktivitu na sociálních sítích vyvíjet nebo nikoliv, resp. je třeba vždy uvážit možné důsledky konkrétní aktivity na sociálních sítích(Král, 2015, s. 172).

Důležitá je rovněž ochrana osobních a identifikačních údajů. Uživatel sociální sítě by si měl jednak ověřit, zda sociální síť uvádí, jakým způsobem jsou osobní údaje zpracovávány, jakým subjektům mohou být případně předávány a jak jsou zabezpečeny. Dále bývá doporučováno neuvádět na sociálních sítích ani své telefonní číslo ani svoji adresu. Obecně platí, že čím méně informací o sobě uživatel na sociální síti uveden, tím menší je pro něj riziko spojené se sociální sítí. Před tím než uživatel cokoliv potvrdí, je třeba si pečlivě přečíst podmínky užívání. Většina sociálních sítí také umožňuje nastavit si soukromí tak, aby informace, které jedinec nechce sdílet zcela veřejně, byly sdíleny jen s omezeným okruhem osob. Je tedy vždy třeba věnovat nastavení soukromí pozornost. Dále je doporučováno nezveřejňovat na sociální síti nic, co uživatel nechce, aby bylo zveřejněno na internetu, popř. by mohlo uživatele nějakým způsobem ohrozit. Typicky se jednoznačně nedoporučuje zveřejňovat například své intimní fotky. Stejně tak je nevhodné takové fotky prostřednictvím sociálních sítí komukoliv zasílat, a to ani osobě, které uživatel důvěřuje, neboť situace se může v budoucnu změnit a ke zneužití může dojít. Stažení takové informace či intimní fotografie z internetu je pak velmi obtížné. Obezřetnost se doporučuje také při používání webové kamery, je totiž nutné předpokládat, že kdokoliv na druhé straně může vše, co kamera přenáší na druhou stranu nahrávat a později také zneužít za různými účely(3).

Další zásadou bezpečnosti na sociálních sítích je nesdělování informací, jako je údaj, kdy je jedinec na dovolené (doporučit lze také sdílet fotografie z dovolené až s odstupem, tj. nejlépe po návratu domů) stejně tak není žádoucí sdělovat například informace o tom, že je člověk nemocný, nemůže se např. z důvodu zranění dobře pohybovat (a tudíž ani bránit případnému útoku) apod. doporučuje se rovněž neodpovídat a nereagovat na vzkazy na sociálních sítích, které jsou hrubé, neslušné či vulgární. V případě, že uživatel s někým komunikovat nechce, popř. je mu komunikace nepříjemná, doporučuje se prostě s takovou osobou nekomunikovat. V případě, že se uživatel na sociální síti setká s nevhodným příspěvkem, obvykle sociální sítě umožňují tento příspěvek nahlásit administrátorovi, který jej následně prověří a případně odstraní. Doporučuje se tedy nevhodné příspěvky vždy nahlásit, aby se zamezilo jejich dalšímu šíření(3).

Pokud je přes internet domlouvána osobní schůzka s člověkem, kterého uživatel nezná, popř. si není jist tím, že je to člověk, za kterého jej uživatel má, je vhodné se vždy sejít na veřejném místě, kde lze předpokládat dostatek lidí a vždy informovat někoho z blízkého okolí, s kým se uživatel schází, na jakém místě a v jakém čase, popř. v kolik hodin předpokládá, že bude zpět. Je možné se také domluvit s někým blízkým, aby uživatele v dohodnutý čas (např. hodinu po setkání) telefonicky kontaktoval a ověřil tak, zda schůzka probíhá bez problémů. Obecně se také doporučuje nevěřit všem informacím, které byly získány skrze sociální sítě, informace je potřeba prověřovat. Samostatnou otázkou je pak zabezpečení uživatelského účtu(3), kterému je věnována následující podkapitola, neboť se k němu vztahuje hned několik různých pravidel a zásad.

3.2.3 Zabepzečení uživatelského účtu na sociálních sítích

Nezbytnou podmínkou bezpečného užívání sociálních sítí je také adekvátní zabezpečení uživatelského účtu na sociálních sítí. To spočívá jednak ve volbě jedinečného uživatelského jména (jímž bývá buď uživatelské jméno, které si jedinec volí, ale velmi často se využívá e-mail uživatele) a také unikátního a silného (bezpečného) hesla k uživatelskému účtu. Vzhledem k tomu, že uživatelské jméno, jímž může být e-mail leckdy ovlivnit uživatel nemůže, je nutné se zaměřit primárně na nastavení dostatečně bezpečného hesla. To znamená, že heslo nesmí být příliš krátké a ani příliš jednoduché (které by se dalo uhádnout). Obvykle se tudíž doporučuje nejméně osm znaků, lépe však deset či více znaků, které heslo tvoří, přičemž je vhodné, aby heslo zahrnovalo alespoň kombinace malých a velkých písmen

s číslovkami, optimálně i další znaky. Heslo by rozhodně nemělo být slovo či kombinace, které lze snadno uhádnout (typicky např. datum narození, místo narození, jméno potomka apod.). vzhledem k tomu, že složité heslo může být ovšem problém si zapamatovat, je optimální si zvolit nějakou větu, kterou si jedinec dokáže zapamatovat a dává mu určitý smysl a z prvních písmen této věty vytvořit základ hesla, který může být dále doplněn také o nějaké číslo, které jedinec dokáže odvodit od informace, kterou si dobře pamatuje. Číslo (popř. jiný znak – např. zavináč, vykřičník apod.) by mělo být zařazeno dovnitř hesla, nikoliv na jeho kraj. Velmi užitečné mohou být rovněž generátory hesel, kde ovšem může opět existovat problém se zapamatováním si nastaveného hesla. Důležité pak také je heslo pravidelně měnit. V literatuře se obvykle doporučuje jej měnit každých 90 dní, nepoužívat neustále tatáž hesla a pokud si jedinec ukládá heslo na svém počítači či ve svém zařízení, je třeba jej ukládat zašifrované(Král, 2015, s. 29), vhodnější však je ukládán hesel na počítači či v mobilním zařízení vůbec nepoužívat.

V této souvislosti je třeba zdůraznit, že člověk by si v žádném případě neměl heslo uložit na cizím zařízení či počítači, jinak hrozí zneužití. Důležité také je heslo k uživatelskému účtu na sociální síti, ale ani k e-mailu, se kterým je účet na sociální síti propojen nesdělovat. Heslo by také nemělo být, pokud možno zapsáno někde, kde se k němu může snadno dostat jiná osoba (např. není vhodné jej mít nalepené na počítači, na nástěnce v práci ani třeba v peněžence, kde může být odcizeno společně s peněženkou).(3).

Nezbytné je také používat kvalitní antivirus, aby nebylo možné heslo získat prostřednictvím infikovaného počítače, z tohoto důvodu je také vhodné vždy zvážit, kde a za jakých okolností se ke svému účtu přihlašovat (například počítač, který není uživatele a není mu dobře znám může být zavirovaný, což může vést i ke krádeži hesla k uživatelskému účtu). Je také vhodné naučit se rozpoznat zavirovaný počítač. Doporučuje se také vždy používat nejaktuálnější verzi internetového prohlížeče a odstraňovat podezřele působící aplikace stejně jako různé doplňky prohlížeče, které mohou ve skutečnosti být cestou, jak zjistit heslo k uživatelským účtům jedince. Stejně tak je nutné být velmi obezřetný, pokud je uživatel např. e-mailem vyzván k zadání hesla ke svému profilu. Leckdy se jedná o falešné e-maily, které usilují právě o získání hesla k účtu, neboť většina solidních sociálních sítí obvykle tímto způsobem zadání hesla po svých uživatelích nepožaduje. Stejně tak se nedoporučuje klikat na podezřelé odkazy

(a to ani tehdy, pokud by působily dojmem, že je zasílá přímo někdo z přátel či sama sociální síť)(4).

Zabezpečení uživatelského účtu však není dáno jen heslem, ale existují i další možnosti. Předně je třeba nastavit si soukromí tak, aby k důležitým informacím měli přístup jen skutečně prověření lidé, zatímco veřejnosti se zobrazovali jen základní informace o uživateli sociální sítě. Řada firem také například výměnou za zpřístupnění určité aplikace vyžaduje zpřístupnění řady údajů z účtu uživatele. Zde je tudíž nutné souhlas se zpřístupněním údajů nedávat a pokud již tak člověk učinil, zkontrolovat komu a jaké údaje zpřístupnil a případně souhlas odebrat (lze obvykle najít v nastavení jednotlivých aplikací)(5).

V případě, že uživatel používá počítač či zařízení, které sdílí s jinými osobami (byť i v rodině), popř. používá například počítač ve veřejných institucích (knihovna, škola apod.), je třeba se vždy důsledně odhlašovat ze svého uživatelského profilu poté, co uživatel ukončí práci na svém profilu. Řada sociálních sítí také v dnešní době nabízí nejrůznější formy nadstandardního zabezpečení, které je vhodné používat. Jedná se například o dvoufázové ověření (např. vedle zadání hesla se člověk musí ještě ověřit prostřednictvím kódu, který je zaslán např. do sms). Je také možné si nastavit automatické zasílání informací o podezřelém přihlášení do profilu (sociální síť např. detekuje, že se člověk přihlásil ze zcela jiné lokality, než se přihlašuje běžně a odešle o tom uživateli notifikaci do e-mailu či do sms)(4).

3.2.4 Vybrané bezpečnostní hrozby na sociálních sítích

Mezi bezpečnostní hrozby, se kterými se lze na sociálních sítích setkat, patří v souladu s tím, co bylo uvedeno již v úvodu práce zejména následující: kyberšikana, kyberstalking, navázání kontaktu s rizikovým jedincem (osobou, která se např. snaží získat osobní informace za účelem jejich zneužití nebo třeba páchání trestné činnosti), počítačové viry, zneužití osobních údajů nebo také krádež identity. Jednotlivá rizika jsou níže podrobněji představena.

Kyberšikanou se rozumí *„záměrné agresivní chování, které je prováděno buď jednotlivcem nebo skupinou prostřednictvím elektronických médií vůči člověku, jenž se v danou chvíli nemůže vůči útokům bránit*.“(Černá, 2013, s. 9*).* Tato agrese či násilí může mít řadu podob. V odborné literatuře se lze dočíst například, že *„kyberšikana spočívá v tom, že se na internetu zveřejňují o oběti pomluvy, nebo i pravdivé, ale choulostivé informace z jejího soukromí,*

včetně obrazového materiálu (v současné době snadno získávaného mobilním telefonem).“(Říčan, Janošová, 2010, s. 24). Charakteristickým rysem kyberšikany je pak také fakt, že zde absentuje asymetrický vztah mezi pachatelem šikany a její obětí, který se běžně při šikaně projevuje tím, že agresor demonstruje svoji převahu a moc. Na internetu je hlavním problémem spíše fakt, že agresor často zůstává skrytý, čímž se internet leckdy stává nástrojem, jehož prostřednictvím se šikany může dopouštět agresor, který zdaleka není silnější než oběť, naopak leckdy se může jednat o jedince slabého. Internet je zde však nástrojem, který může šikanu zásadním způsobem umocňovat.[1]Tím je dán i fakt, že ačkoliv se situace může jevit tak, že se vše odehrává pouze ve virtuálním prostředí, tedy kyberšikana není tak závažná jako jiné formy šikany, opak je pravdou. Může být nejen stejně závažná, ale dokonce i závažnější(Černá, 2013, s. 9).

Kyberstalking lze chápat jako opětovné zasílání nevyžádaných zpráv, které obvykle obsahují výhrůžky, zastrašující či útočná sdělení, případně také vydírání. Kybestalking může v některých případech přejít rovněž ve fyzické ohrožení oběti, přičemž obvykle bývá toto fyzické ohrožení nejprve součástí obsahu vyhrůžek, které agresor oběti prostřednictvím sociálních sítí směřuje(Černá, 2013, s. 26). Pro kyberstalking je dále charakteristické, že dochází k opakovanému narušování bezpečnosti a soukromí oběti. Paradoxní je, že kyberstalker nejprve obvykle oběti opakovaně a poměrně intenzivně projevuje přízeň, nicméně posléze se situace změní a dochází naopak k výhrůžkám a zastrašování oběti(Pugnerová, Kvintová, 2016, s. 100).

Navázání kontaktu s rizikovým jedincem, jehož cílem je obvykle dopouštění se nějaké formy kriminální činnosti, a který obvykle za účelem navazování těchto kontaktů používá fiktivní účet, je rizikem především proto, že jedinec s fiktivním účtem se po přidání do seznamu kontaktů (navázání přátelství na sociální síti) dozvídá řadu informací o své oběti. Může tak snadno zjistit například, kdy jede oběť na dovolenou, aby mohl v daném období vykrást byt oběti, může pod různými záminkami vylákat z oběti řadu informací (i osobního a intimního charakteru, popř. třeba fotografií intimního rázu), které později využije za účelem vydírání. Stejně tak je možné vysledovat z profilu na sociálních sítí určité zákonitosti fungování oběti, čímž je možné například zjistit, kde se pohybuje, kde pracuje, kde bydlí, kdy bývá a nebývá doma, zda má děti apod. Zde pak vzniká prostor jak pro vydírání, tak například

pro naplánování únosu či zneužití informací například za účelem ohrožení kariéry apod. Velmi často je falešný účet používán například za účelem navázání dospělého jedince s dítětem či dospívajícím jedincem, třeba právě z účelem vylákání intimních fotografií, popř. za účelem zneužití dítěte. Zde se často dospělý vydává za vrstevníka oběti, čímž je dítěte či dospívajícímu jedinci méně podezřelý. Využití falešného profilu, za kterým stojí rizikový jedinec s nekalými, popř. i nezákonnými cíli je zásadním rizikem, neboť i odborná literatura poukazuje na skutečnost, že vytvořit falešný profil na sociálních sítích je velmi jednoduché, proto jich je na sociálních sítích poměrně velké množství a je vždy dobré prověřovat, koho si do seznamu kontaktů („přátel“) jedinec přidává.[2] Fiktivní účet však nemusí vždy sloužit jen k trestné činnosti, někdy může být použit například jako žert, nicméně tento fakt nic nemění na skutečnosti, že při přidávání osob, s nimiž si jedinec není jist, že se skutečně zná, je třeba být velmi obezřetný(Pospíšilová, 2016, s. 12).

Počítačové viry jsou tradičním problémem spojeným s používáním informačních technologií a internetu. Virem se obvykle rozumí program, který se šíří bez vědomí uživatele počítače. Tím je virus také tak problematický, neboť uživatel leckdy vůbec neví o tom, že jeho počítače je zavirovaný a viry šíří dále. Virus je přitom rizikem především proto, že je svým tvůrcem obvykle vytvořen buď za účelem toho, aby zničil počítač uživatele nebo aby odcizil některá data v počítači (kterými mohou být například i hesla k e-mailovým i dalším účtům stejně jako třeba údaje o platebních kartách, které uživatel používá k nákupům přes internet(Procházka, 2010, s. 18). Na sociálních sítích se leckdy viry šíří tak, že se tváří například jako vzkazy od lidí, které má jedinec v přátelích, popř. jako odkaz, který je bez vědomí uživatele, který má zavirovaný počítač sdílen na jeho profilu a vybízí ke kliknutí na něj, podobně se může šířit také jako obrázek, popř. příloha. Poté, co na takový obrázek či soubor jedinec klikne, virus napadne jeho počítač a zároveň začne rozesílat vzkazy dalším uživatelům, které má tento člověk v přátelích na sociální síti(6).

Zneužití osobních údajů je jedním z dalších významných rizik spojených s používáním sociálních sítí, neboť již z profilu uživatele je možné řadu osobních údajů zjistit, další osobní údaje leckdy jedinec neuváženě sdělí např. do vzkazů při komunikaci s rizikovým jedincem. Výsledkem pak může být řada různých forem zneužití osobních údajů. Stejně tak je možné některé osobní údaje ze sociálních sítí získat také prostřednictvím virů, ale v řadě případů je

uživatel, aniž by pořádně četl veškeré podmínky a informace o tom, s čím uděluje souhlas, sdělí své osobní údaje z profilu třetí straně. Zneužití osobních údajů pak může mít řadu podob, od jejich distribuce dalším subjektům, kteří pak jedince obtěžují nevyžádanými nabídkami, přes neoprávněný vstup do cizí e-mailové schránky a rozesílání sdělení (leckdy nevhodných, nevyžádaných apod.) jménem uživatele, jehož osobní údaje jsou zneužívány, stejně tak mohou být osobní údaje využity např. k zakládání profilů na řadě míst (typicky např. seznamky, pornografické servery apod.). S přístupem k osobním údajům se leckdy může nežádoucí osoba dostat rovněž k seznamu přátel, které může např. obtěžovat nevyžádanými sděleními, popř. se vydávat za toho, jehož osobní údaje jsou zneužity (z různých důvodů). Dojít může i ke zneužití údajů k platebním nástrojům, které jsou využity k cizím nákupům apod. Velmi závažnou formou zneužití osobních údajů může být také krádež identity(Kopecký, Krejčí, 2010, s. 9).

Krádež identity může mít hned několik podob. Policie ČR v zásadě poukazuje na celkem tři možnosti krádeže identity, a to na: finanční krádež identity, kriminální krádež identity a rovněž krádež identity, jejímž cílem je vytvoření zcela nové identity. *„Největší nebezpečí představuje finanční krádež identity, kdy podvodník zneužije citlivé osobní údaje oběti pro přístup k bankovnímu účtu, kreditní kartě a má možnost si tak pronajmout v půjčovnách auta, která zpětně už nevrátí, nakupovat zbraně, objednávat si hotelové pokoje a za své služby neplatit, uzavírat různé smlouvy apod.“(7).* Další možností je kriminální krádež identity, jejíž podstata spočívá v tom, že jedinec využívá cizí osobní údaje za účelem spáchání nějakého trestného činu pod cizím jménem. Poslední možností je pak krádež identity, která směřuje k vytvoření zcela nové identity jedince a možnosti začít žít někde jinde pod zcela novým jménem (s novou identitou). Typicky se jedná o krádež identity spojenou s vyhýbáním se trestnímu stíhání, popř. postihu(7).

3.3 Bezpečnostní skandály

3.3.1 Bezpečnostní skandály

Mezi nejvýznamnější bezpečnostní skandály poslední doby se určitě řadí sdílení osobních údajů třetím stranám. Jedna z největších sociálních sítí na světě – Facebook sama čelí skandálu, kdy vědomě poskytovala osobní data svých uživatelů až 60 výrobcům telefonů včetně značek Samsung, Apple, Lenovo a další, ale také Huawei kterou americké úřady považují za hrozbu pro národní bezpečnost(8).

To ovšem není jediný skandál, kterému společnost Facebook čelí.

Na začátku roku 2018 vypukl skandál, poté co vyplulo na povrch, že společnost Cambridge America, získala osobní data milionů uživatelů bez jejich souhlasu, které následně využila k politickým účelům. Únik dat se týkal až 50 milionů uživatelů, většinově amerických občanů. Celý skandál měl dohru svědectvím zakladatele společnosti Marka Zuckerberga před americkým Kongresem.

3.3.2 Nařízení GDPR

Nejenom v důsledku bezpečnostních skandálů s úniky osobních dat uživatelů, Evropská Unie představila obecné nařízení o ochraně osobních údajů neboli GDPR.

„*GDPR* *představuje nový právní rámec ochrany osobních údajů v evropském prostoru s cílem hájit co nejvíce práva občanů EU proti neoprávněnému zacházení s jejich daty včetně osobních údajů. GDPR se týká všech firem a institucí, ale i jednotlivců a online služeb, které zpracovávají data uživatelů. GDPR zavedlo astronomické pokuty za porušování pravidel a nařizuje některým správcům nebo zpracovatelům osobních údajů zřídit nezávislou kontrolní funkci* ***DPO*** *(*Data Protection Officer*, tj. Pověřenec pro ochranu osobních údajů)*“(9).

Dalším důvodem pro zavedení nařízení GDPR, byla zjištění, že výzvědné služby zemí mimo Evropskou Unii v minulosti shromaždovali informace o občanech EU.

4 VLASTNÍ PRÁCE

V návaznosti na teoretická východiska, která byla představena v předcházejících kapitolách byl realizován rovněž vlastní výzkum. Za účelem prezentace výsledků je kapitola rozdělena na dvě části, kdy první analyzuje otázky, jejichž cílem bylo získat charakteristiku výzkumného souboru a druhá se zaměřuje na vyhodnocení otázek dotazníkového šetření, které se týkaly přímo tématu, tedy bezpečnosti na sociálních sítích a souvisejících hrozeb.

4.1 Charakteristika výzkumného souboru

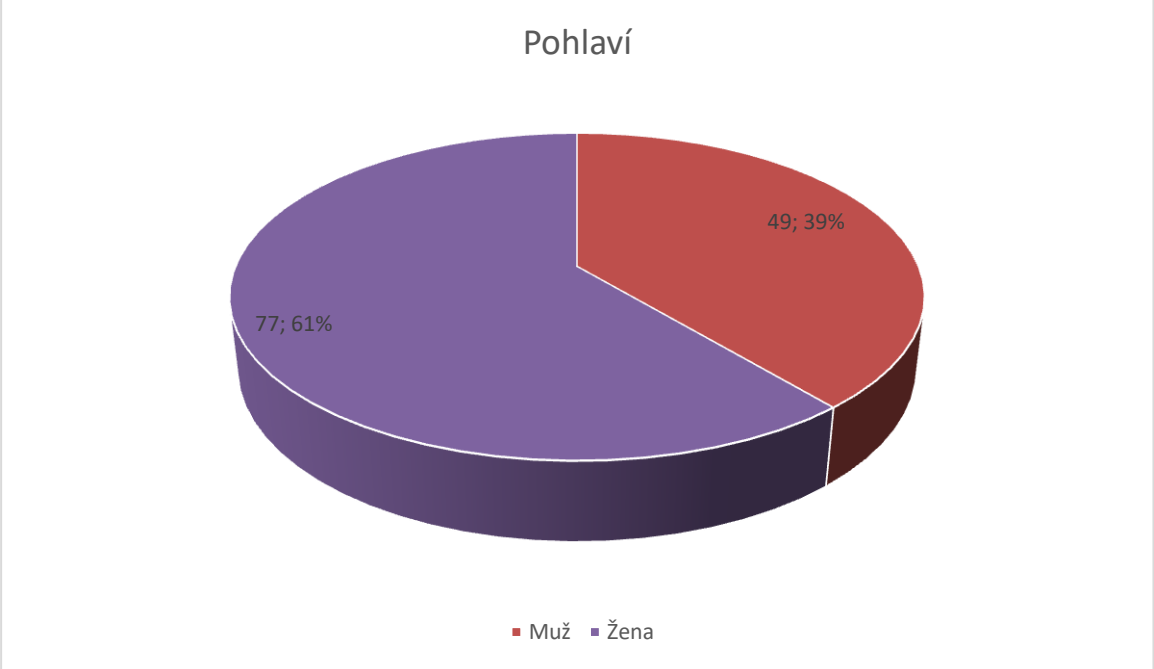
Jak již bylo zmíněno v metodice, dotazník celkem vyplnilo 126 osob, které byly zařazeny do vyhodnocení výsledků. 126 osob tedy tvoří 100 % výzkumného souboru. Vzhledem k tomu, že uživateli sociálních sítí jsou zejména mladší generace, byl výzkum cílen na jedince ve věku

18-35 let žijící v hlavním městě Praze a Středočeském kraji. Tento fakt respondenti při vstupu do dotazníkového šetření museli odsouhlasit, aby se jim zobrazil vlastní dotazník, následně pak byly zjišťovány podrobnosti ohledně charakteristik výzkumného souboru, které jsou následující:

Otázka č. 1: Jste?

První otázka zaměřená na charakteristiku výzkumného souboru zjišťovala, jaké je pohlaví respondentů. Je zřejmé, že dotazníku se zúčastnilo více žen, které tvořili 61 % (77) výzkumného souboru než mužů, kteří tvořili jen 39 % (49) respondentů v rámci výzkumného souboru. Strukturu respondentů dle pohlaví znázorňuje rovněž graf č. 1.

Graf č. 1: Pohlaví respondentů

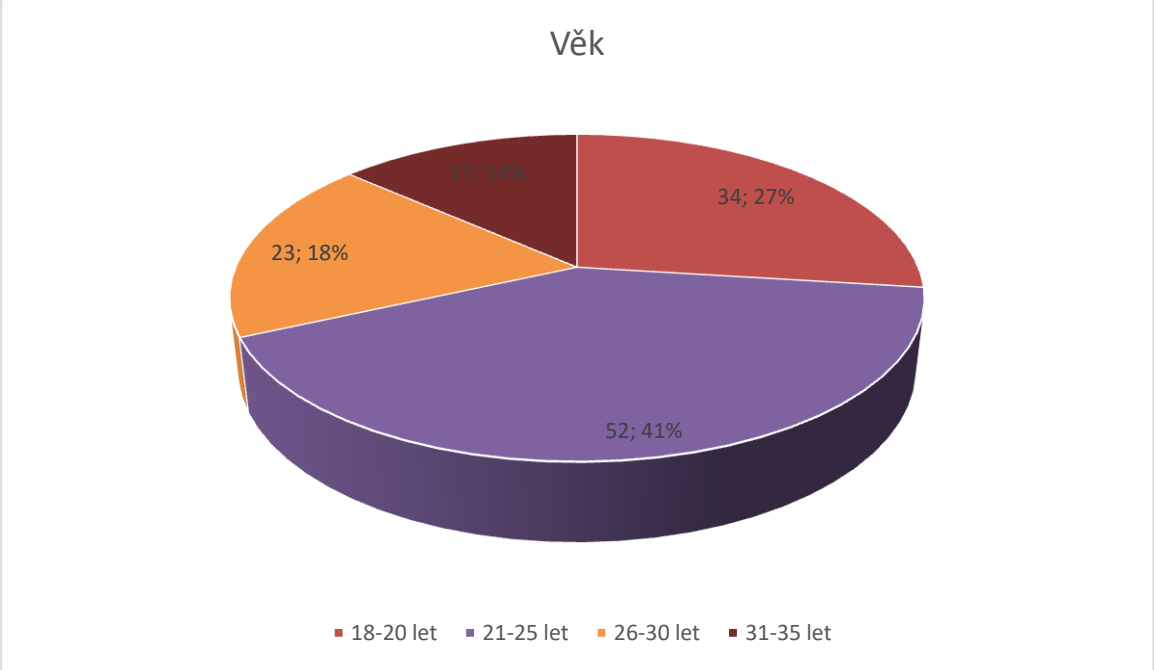


Zdroj: Vlastní výzkum

Otázka č. 2: Kolik je Vám let?

Ačkoliv na samotném počátku dotazníku bylo nutné potvrdit, že respondent patří do kategorie respondentů ve věku 18-35 let, tato otázka pak tuto kategorii dále členila a zjišťovala bližší údaje. Ukázalo se, že ve výzkumu i v této věkové kategorii převažovali zejména lidé nižšího věku, neboť 41 % (52) respondentů tvořili lidé ve věku 21-25 let, 27 % (34) respondentů tvořili lidé ve věku 18-20 let, 18 % (23) respondentů tvořili lidé ve věku 26-30 let a zbývajících 14 % 17) respondentů tvořili lidé ve věku 31-35 let, což svědčí o tom, že jednoznačně převažovali lidé ve věku do 25 let, ostatních bylo ve výzkumné souboru výrazně méně. Struktura výzkumného souboru dle věku je znázorněna v grafu č. 2.

Graf č. 2: Věk respondentů

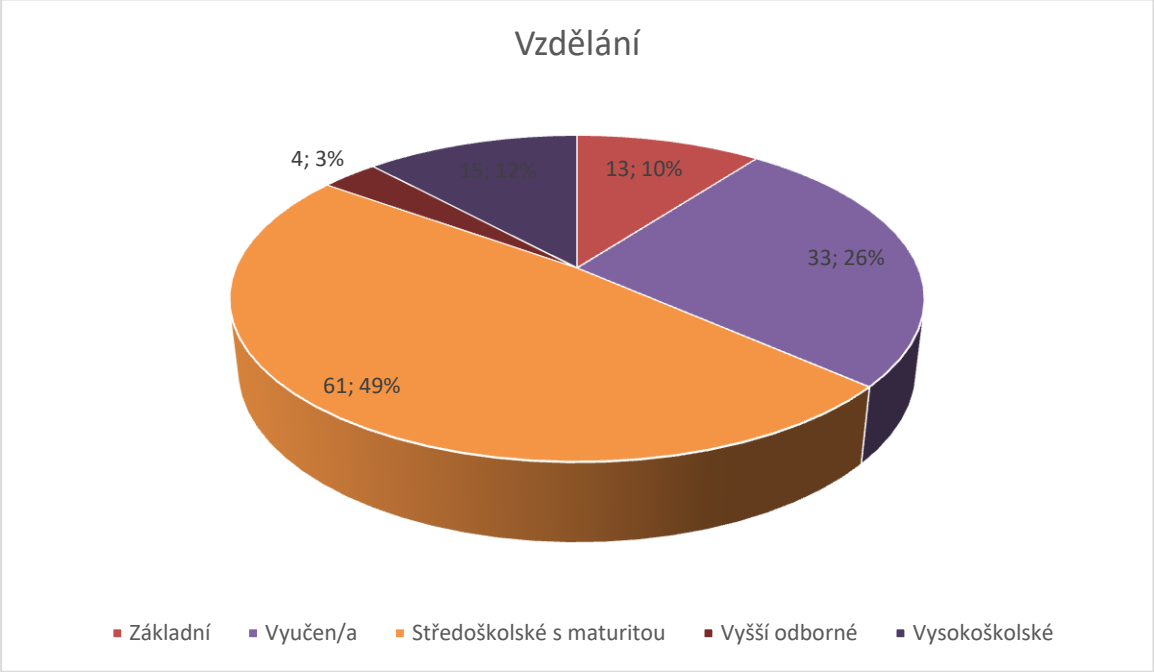


Zdroj: vlastní výzkum

Otázka č. 3: Jaké je Vaše nejvyšší dosažené vzdělání?

Z otázky zjišťující nejvyšší dosažené vzdělání respondentů vyplynulo, že 49 % (61) respondentů mělo středoškolské vzdělání s maturitou, 26 % (33) respondentů bylo vyučených, 12 % (15) respondentů mělo vysokoškolské vzdělání, 10 % (13) respondentů mělo základní vzdělání a 3 % (4) respondentů měla vyšší odborné vzdělání. Na vyšší výskyt nižšího vzdělání (zejména základního) měl patrně vliv i fakt, který plynul jak z charakteristiky věkové struktury výzkumného souboru, tak z otázky č. 5, a to fakt, že řada respondentů zejména v mladších věkových kategoriích doposud studuje. Výsledky odpovědí na tuto otázku představuje graf č. 3.

Graf č. 3: Vzdělání

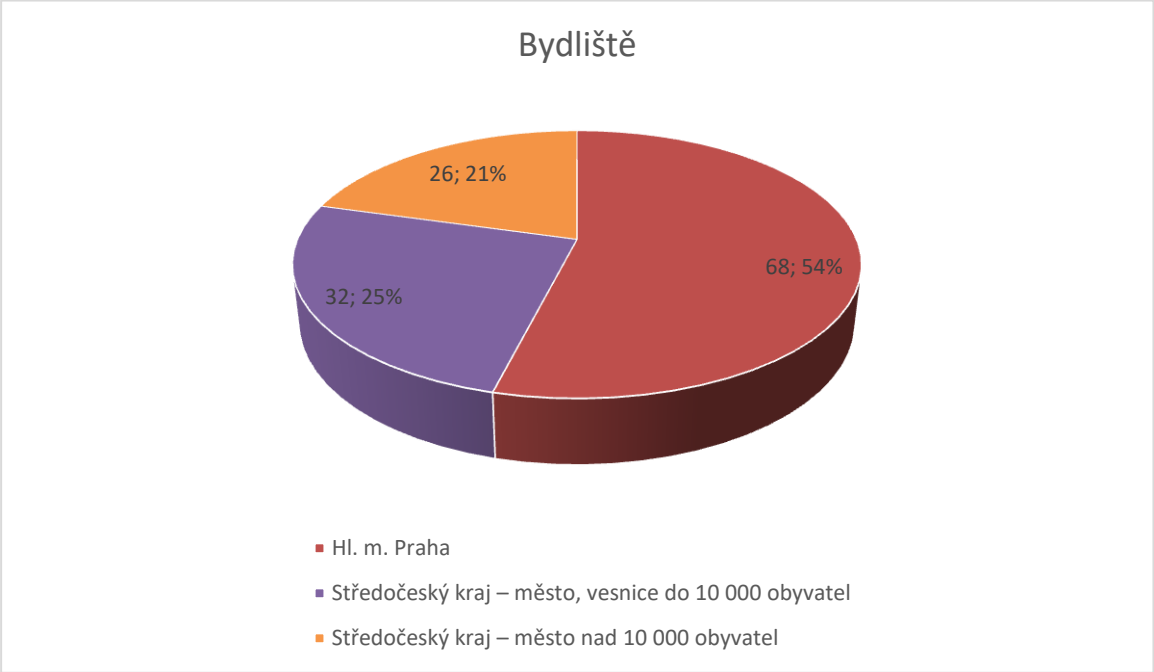


Zdroj: vlastní výzkum

Otázka č. 4: Kde žijete?

Vzhledem k tomu, že dotazník byl určen jen respondentům z Prahy a Středočeského kraje, což respondenti na počátku stvrzovali, jinak vůbec nebyly připuštěni k vyplňování dotazníku, bylo zjišťování zaměřeno především na to, zda respondent žije ve větším městě nebo na malém městě, popř. vesnici. V návaznosti na tuto otázku se podařilo zjistit, že 54 % (68) respondentů žilo v hlavním městě Praze, dalších 25 % (32) respondentů žilo ve městě, popř. vesnici do 10 000 obyvatel ve Středočeském kraji a zbývajících 21 % (26) respondentů uvedlo, že žije ve městě nad 10 000 obyvatel ve Středočeském kraji. Výsledky odpovědí na tuto otázku charakterizující výzkumný soubor představuje graf č. 4.

Graf č. 4: Místo bydliště

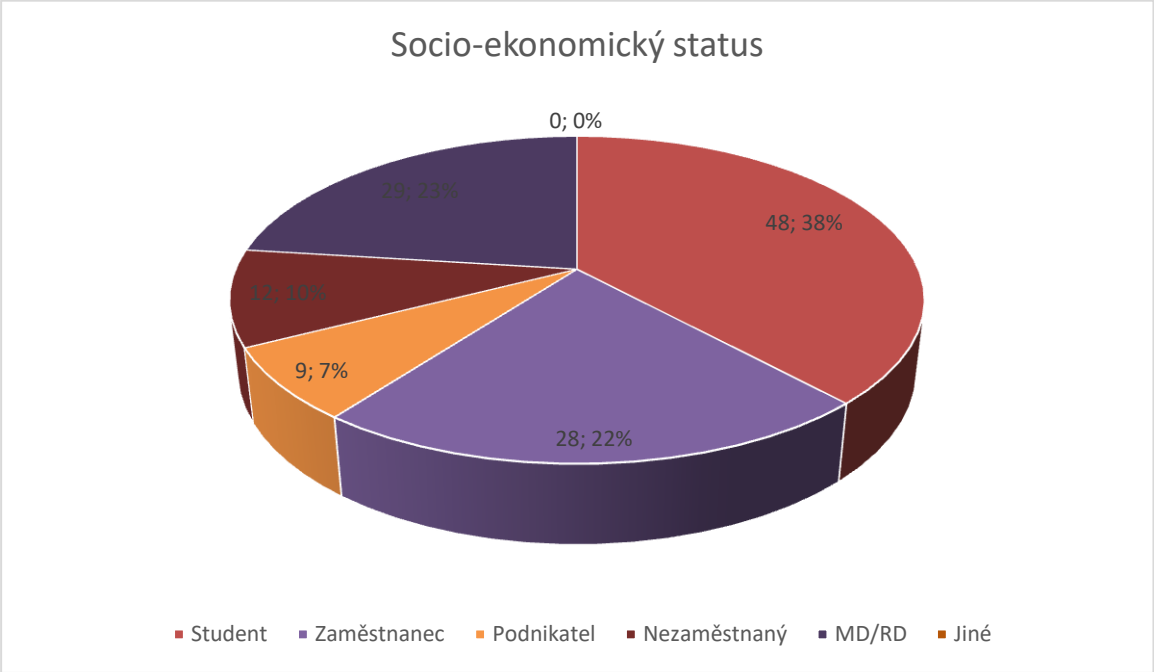


Zdroj: vlastní výzkum

Otázka č. 5: Jaký je váš socio-ekonomický status?

Tato otázka zjišťovala, jaký je socio-ekonomický status respondentů ve výzkumném souboru. Jak bylo již výše zmíněno, nejpočetnější skupinu respondentů, a to 38 % (44) respondentů tvořili studenti, 23 % (29) respondentů tvořili lidé na mateřské, popř. rodičovské dovolené, 22 % (28) respondentů představovali lidé zaměstnaní, 10 % (12) respondentů představovali lidé nezaměstnaní, 7 % (9) respondentů pak tvořili podnikatelé. Výsledky odpovědí na tuto otázku představuje graf č. 5.

Graf č. 5: Socio-ekonomický status



Zdroj: vlastní výzkum

Vyhodnocení dotazníkového šetření

Vlastní vyhodnocení dotazníkového šetření je rozděleno na dvě části, které v souladu se strukturou dotazníku nejprve vyhodnocují obecně informace týkající se užívání sociálních sítí ze strany respondentů a druhá část se pak zaměřuje konkrétně na bezpečnost a rizika spojená se sociálními sítěmi.

4.2.1 Zkušenost a používání sociálních sítí z pohledu respondentů

Obecnější informace o tom, jaké mají respondenti zkušenosti a znalosti o sociálních sítích, byly zjišťovány prostřednictvím následujících otázek:

Otázka č. 6: Založil/a jste si někdy profil na některé ze sociálních sítí (byť třeba i jen na zkoušku, který třeba nyní ani nevyužíváte)?

Z odpovědi na tuto otázku vyplynulo, že 99 % (125) respondentů si někdy v životě alespoň na zkoušku založilo profil na sociální síti. Jen 1 % (1) respondentů tak nikdy v životě neučinilo. Graficky je odpověď na tuto otázku znázorněna v grafu č. 6.

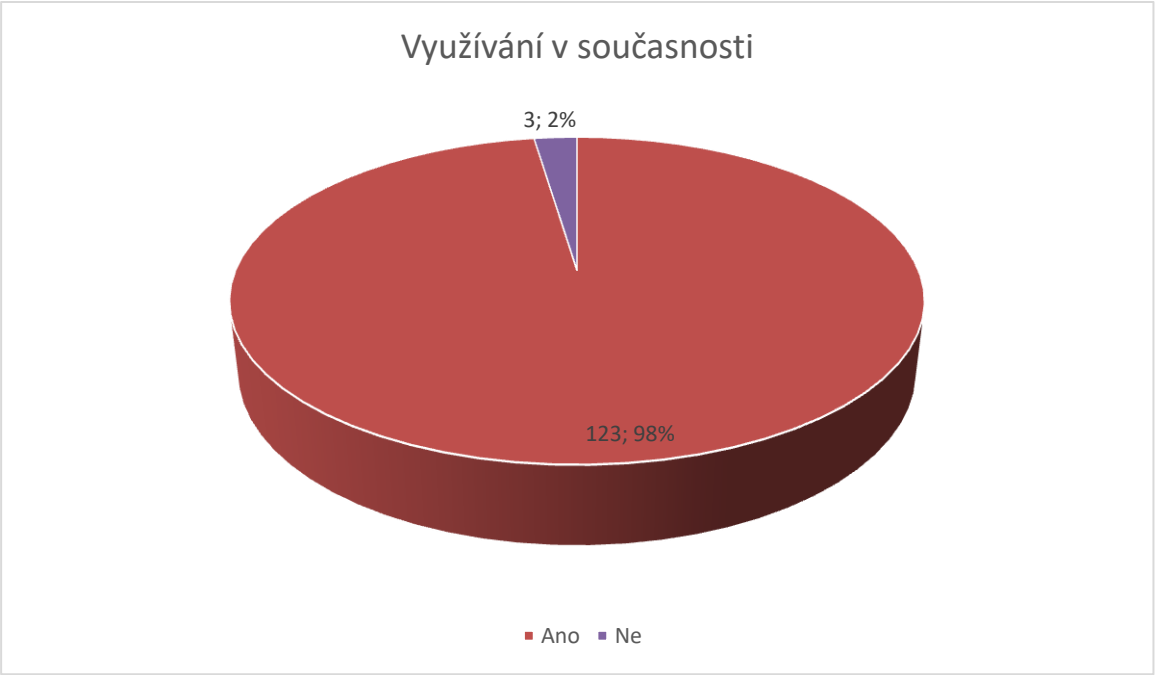
Graf č. 6: Založení profilu na sociální síti

Zdroj: vlastní výzkum

Otázka č. 7: Využíváte v současné době některou ze sociálních sítí?

Z odpovědí na tuto otázku vyplynulo, že 98 % (123) respondentů v současné době nějakou sociální síť využívá, jen 2 % (3) respondentů uvedla, že nikoliv. Odpovědi na tuto otázku jsou zaneseny do grafu č. 7.

Graf č. 7: Využívání sociální sítě v současnosti



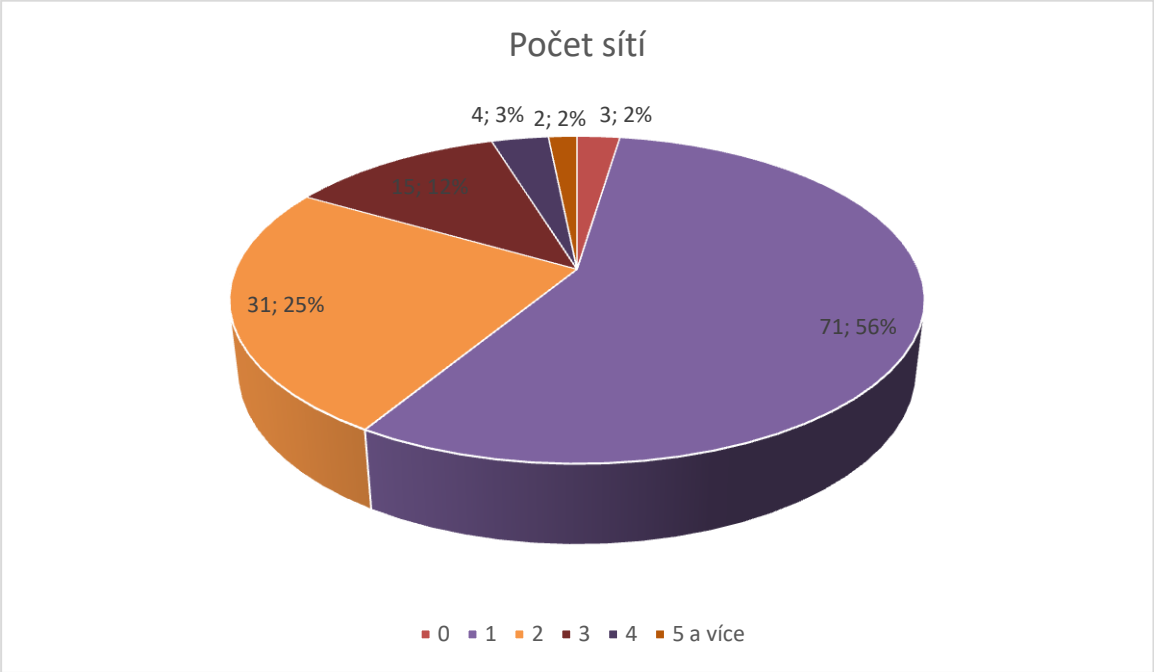
Zdroj: vlastní výzkum

Z obou předcházejících odpovědí tedy jednoznačně vyplynulo, že naprostá většina respondentů má zkušenosti se sociálními sítěmi. V této souvislosti stojí také za zmínku, že ti respondenti, kteří tyto zkušenosti neměli, popř. aktuálně žádnou sociální síť nepoužívali, byli ve výzkumu ponecháni zejména proto, že i tito lidé mohou například projevit o sociální sítě zájem v budoucnu, zjistit tak jejich znalosti a pohled na otázky bezpečnosti je žádoucí, byť u některých otázek přínos jejich odpovědí nebude tak velký jako u respondentů, kteří sociální sítě používají aktivně.

Otázka č. 8: Kolik sociálních sítí v současnosti využíváte?

Z odpovědí na tuto otázku vyplynulo, že 56 % (71) respondentů využívá v současné době jednu sociální síť, 25 % (31) uvedlo, že využívají dvě sociální sítě, 12 % (15) respondentů pak využívalo tři sociální sítě. Ostatní odpovědi již byly výrazně méně časté, neboť 3 % (4) respondentů uvedla, že využívají čtyři sociální sítě, 2 % (2) respondentů pak uvádělo dokonce pět nebo více sociálních sítí a další 2 % (3) respondentů uvedla, že nevyužívají v současné době žádnou sociální síť. Výsledky odpovědí na tuto otázku jsou znázorněny v grafu č. 8.

Graf č. 8: Počet aktuálně používaných sociálních sítí

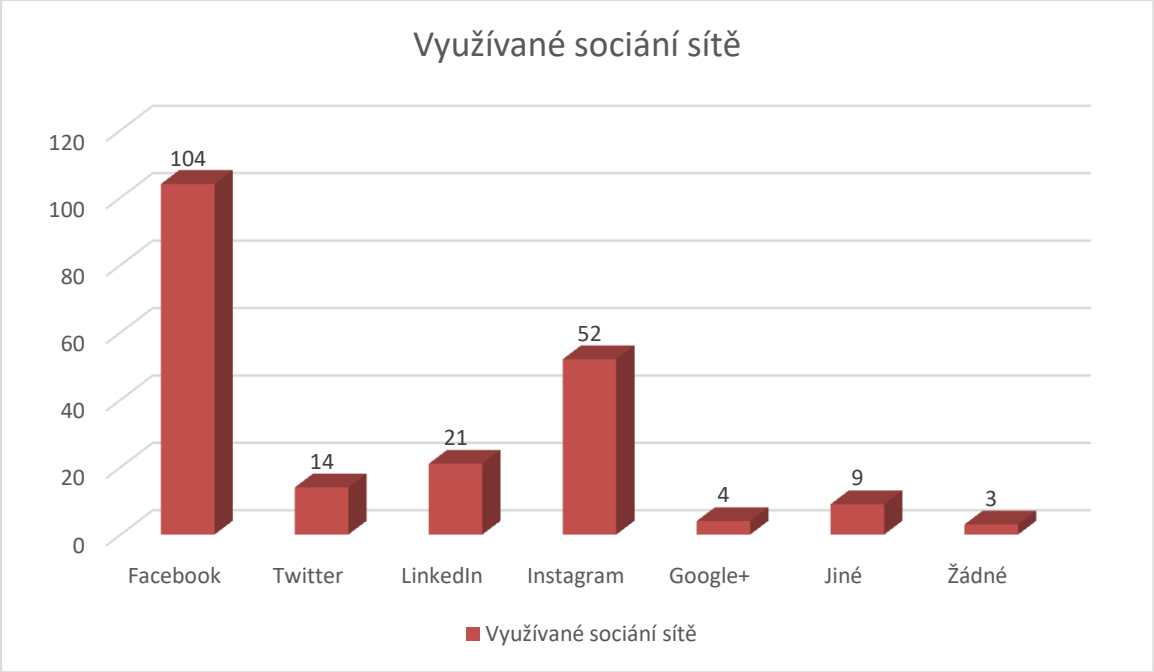


Zdroj: vlastní výzkum

Otázka č. 9: Které z následujících sociálních sítí využíváte?

Na otázku, které sociální sítě respondenti používají, bylo možné uvést libovolný počet odpovědí, neboť jak je zřejmé již z otázky předcházející, řada respondentů používá více než jednu sociální síť. Z tohoto důvodu jsou za účelem vyhodnocení použity sloupcové grafy a vyhodnocení je realizován za pomocí absolutních čísel, nikoliv procentuálního vyjádření. Z výsledků, které znázorňuje graf č. 9 je patrné, že jednoznačně nejvíce respondentů využívalo sociální síť Facebook, který využívalo 104 respondentů, druhou nejčastěji využívanou sociální sítí byl pak Instagram, který zmínilo 52 respondentů. Využití ostatních sociálních sítí bylo již výrazně méně četné, nicméně 21 respondentů zmínilo LinkedIn, 14 respondentů Twitter, 9 respondentů jiné (objevilo se zde zejména Flickr, Pinterest či Tumnlr). Jen čtyři respondenti pak uvedli, že používají Google + a v návaznosti na zjištění předchozích otázek tři respondenti uvedli, že nepoužívají žádnou sociální síť.

Graf č. 9: Využívané sociální sítě



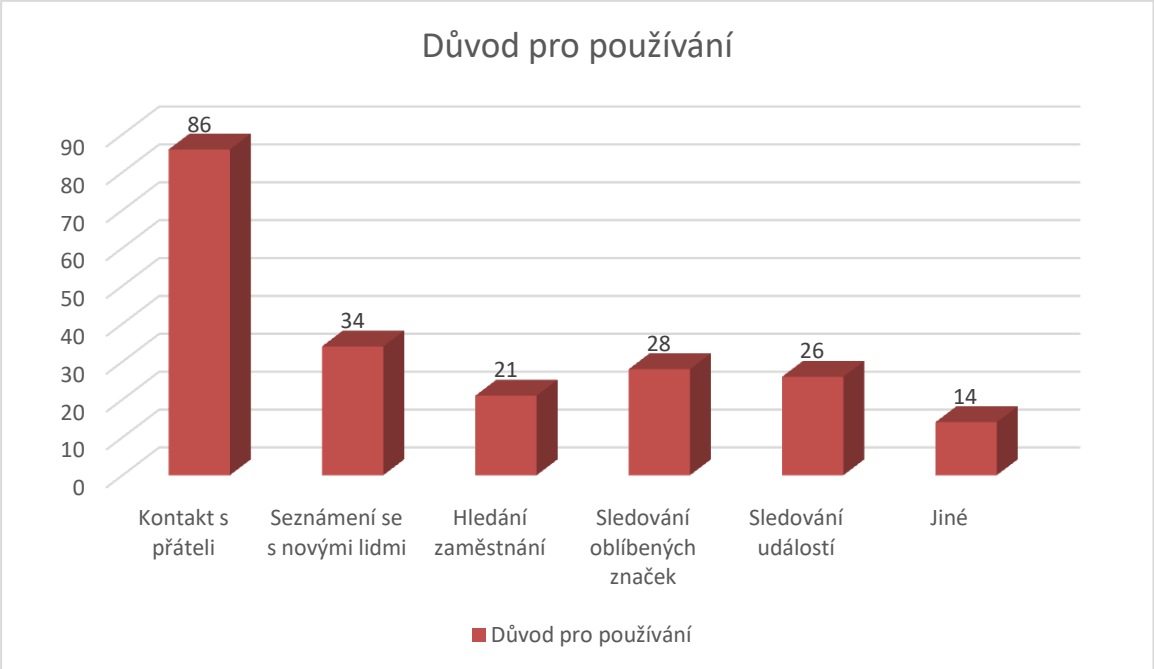
Zdroj: vlastní výzkum

Otázka č. 10: Z jakých důvodů sociální sítě využíváte? (Pokud sociální sítě nevyužíváte, zvolte důvod(y), pro který byste je nejspíše využívat byli ochotni začít).

Desátá otázka dotazníku pak zjišťovala, z jakých důvodů respondenti sociální sítě využívají, u těch, kteří je nevyužívají, měl být zvolen důvod, pro který by je nejspíše začali využívat, přičemž i u této otázky bylo možné zvolit více variant odpovědí, tudíž jsou opět výsledky znázorněny v grafu č. 10 pomocí sloupcových grafů a jsou vyhodnoceny v absolutních číslech.

Z odpovědí respondentů vyplynulo, že nejčastěji sociální sítě využívají za účelem kontaktu s přáteli, což je odpověď, kterou uvedlo 89 respondentů. Dalších 34 respondentů zmínilo, že sociální sítě využívá také za účelem seznámení se s novými lidmi. 28 respondentů pak sociální sítě využívá za účelem sledování svých oblíbených značek a produktů, 26 respondentů uvedlo také sledování událostí, 21 respondentů uvedlo, že důvodem pro používání sociálních sítí je pro ně hledání zaměstnání a 14 respondentů uvedlo jiný důvod, kde respondenti vypisovaly například sdílení fotografií, sledování inzertních a bazarových skupin, telefonování zdarma a další důvody, proč sociální sítě využívají. Je tedy zřejmé, že možností, proč se lidé rozhodnou sociální sítě využívat je v dnešní době nespočet a každému může využívání sociální sítě přinášet jiné benefity.

Graf č. 10: Důvody pro využívání sociálních sítí



Zdroj: vlastní výzkum

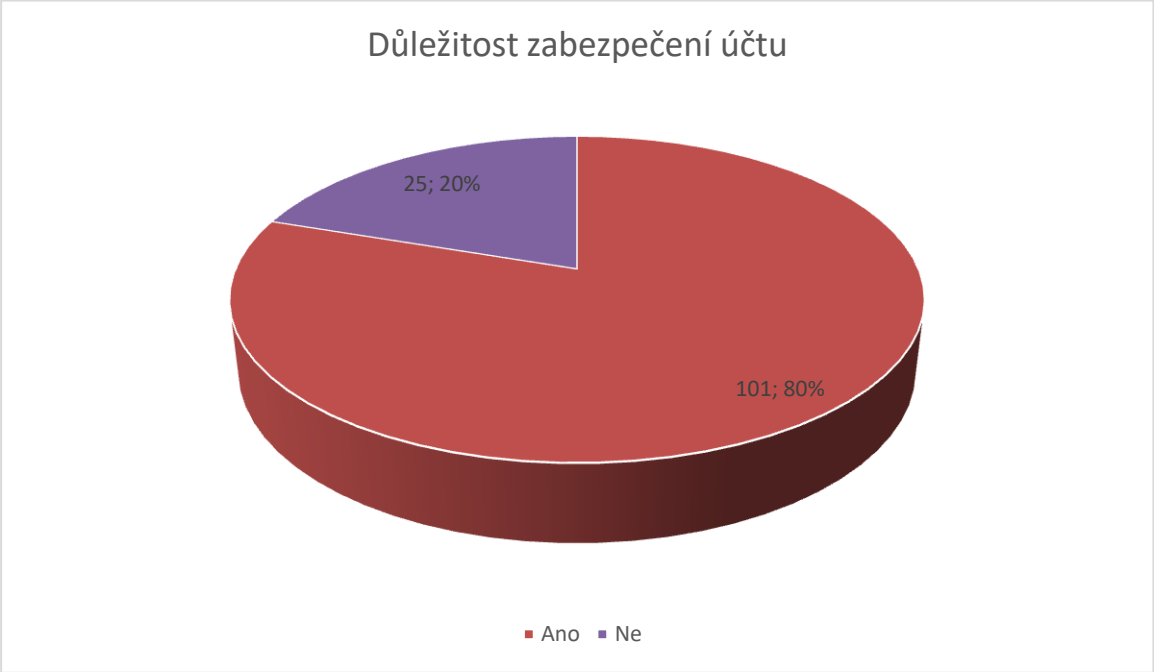
4.2.2 Bezpečnost a bezpečnostní hrozby na sociálních sítích z pohledu respondentů

Nejpočetnější skupinu otázek v dotazníku tvořily otázky, které se zaměřovaly přímo na bezpečnost na sociálních sítích, zabezpečení uživatelského účtu a na bezpečnostní hrozby, které jsou s užíváním sociálních sítí spojeny. Tyto aspekty byly analyzovány za pomocí následujících otázek:

Otázka č. 11: Je pro Vás důležité, aby váš účet na sociálních sítích byl dostatečně zabezpečen?

Z odpovědí respondentů na tuto otázku vyplynulo, že pro 80 % (101) respondentů bylo důležité, aby byl jejich účet na sociálních sítích dostatečně zabezpečen, zatímco pro 20 % (25) respondentů tento fakt důležitý nebyl. Graficky je výsledek odpovědí na tuto otázku znázorněn v grafu č. 11, který je přiložen.

Graf č. 11: Důležitost zabezpečení účtu



Zdroj vlastní výzkum

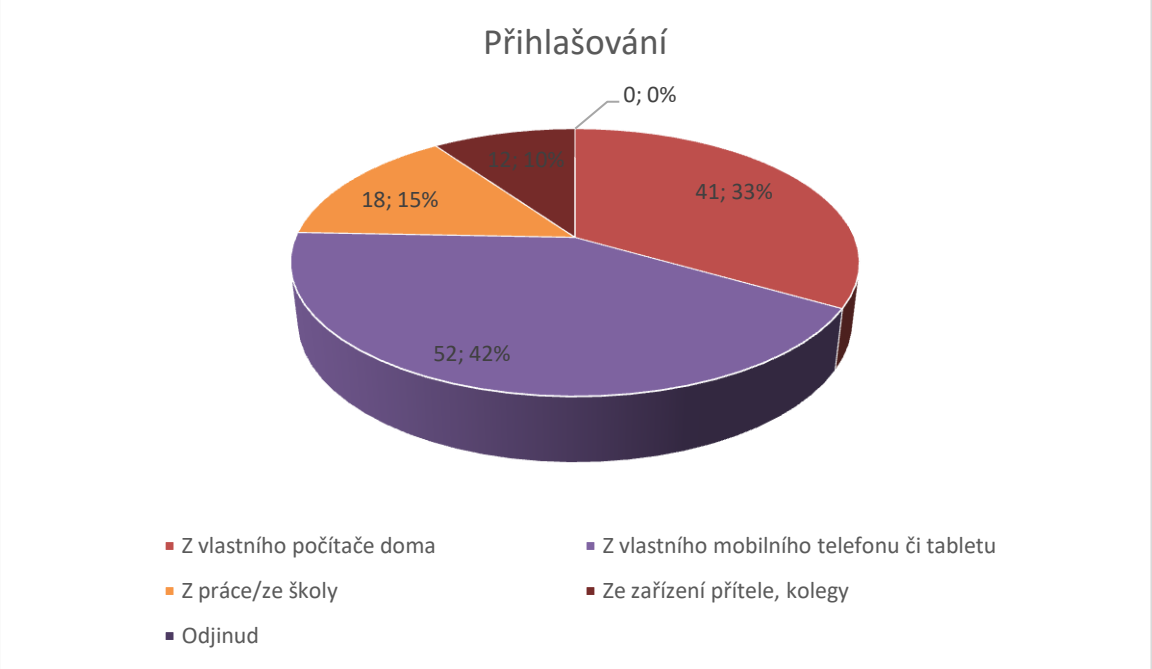
Tato otázka byla koncipována jako obecná a úvodní do třetí části dotazníku, ostatní otázky pak již byly zaměřeny konkrétněji na nejrůznější formy zabezpečení účtu, přihlašovacích údajů stejně jako na vybrané bezpečnostní hrozby. Od odpovědí na tuto otázku se však mohou odvíjet i odpovědi na další otázky, tudíž otázka zcela jistě svůj význam v dotazníku má. Vzhledem k tomu, že další otázky zjišťovaly, jakým způsobem se respondenti chovají na

sociálních sítích, vyplňovaly je dále jen ti, kteří sociální sítě používají, tedy 123 respondentů, kteří tvořili 100 % výzkumného souboru.

Otázka č. 12: Odkud se k sociální síti nejčastěji přihlašujete?

Z odpovědí na tuto otázku vyplynulo, že nejpočetnější skupina, a to 42 % (52) respondentů se k sociálním sítím přihlašuje z vlastního telefonu, případně z tabletu. Druhá nejpočetnější skupina tvořená 33 % (41) respondentů uvedla, že se nejčastěji přihlašuje z vlastního počítače, který mají respondenti doma. 15 % (18) respondentů pak uvedlo, že se nejčastěji přihlašují z počítače v práci, popř. ve škole a zbývajících 10 % (12) respondentů se nejčastěji přihlašovalo ze zařízení přítele či kamaráda, popř. obecně jiné osoby. Jiná varianta nebyla zmíněna. Výsledky odpovědí na tuto otázku jsou znázorněny v grafu č. 12.

Graf č. 12: Zařízení nejčastějšího přihlášení



Zdroj: vlastní výzkum

Otázka č. 13: Ukládáte si hesla k profilům na sociální sítě do počítače či jiného zařízení, odkud se k sociální síti přihlašujete?

Z odpovědí na výše uvedenou otázku vyplynulo, že celých 79 % (97) respondentů si do zařízení, na kterém se pravidelně přihlašují k sociální síti, ukládají heslo ke svému účtu na sociální síti. To je přitom z bezpečnostního hlediska jedním z poměrně významných rizik. Pouze 21 % (26) respondentů uvedlo, že si hesla do zařízení neukládá. Výsledky odpovědí na tuto otázku představuje graf č. 13.

Graf č. 13: Ukládání hesel do zařízení

Zdroj: vlastní výzkum

Otázka č. 14: Máte nastavené bezpečné heslo splňující následující požadavky: alespoň osm znaků, kombinace malých a velkých písmen s čísly, popř. i dalšími znaky?

Čtrnáctá otázka se zaměřovala na zjištění, zda mají respondenti nastavené heslo k profilu na sociální síti, které lze dle pravidel uvedených v odborné literatuře i teoretické části této práce označit za bezpečné. Z odpovědí respondentů však vyplynulo poměrně znepokojivé zjištění, že 83 % (102) respondentů uvedlo, že bezpečné heslo dle uvedených pravidel nastaveno nemá, jen 17 % (21) respondentů bezpečné heslo při používání sociálních sítí nastaveno má. Výsledky odpovědí na tuto otázku prezentuje graf č. 14.

Graf č. 14: Bezpečné heslo

Zdroj: vlastní výzkum

Otázka č. 15: Máte své heslo napsané někde, kde by se k němu eventuálně mohl dostat jiný člověk (např. v diáři, u počítače, z druhé strany telefonu apod.).

Patnáctá otázka se zaměřovala na další aspekt zabezpečení uživatelského účtu, a to na skutečnost, zda má respondent heslo k účtu na sociální síti napsané někde, kde by se k němu za určitých okolností mohl dostat i jiný člověk. Z výsledků vyplynulo, že naprostá většina respondentů, a to 89 % (109) respondentů heslo někde takto napsané skutečně mělo, jen 11 % (14) respondentů nikoliv. I zde je tudíž patrné, že zabezpečení účtů není pojato optimálně. Výsledky odpovědí na tuto otázku prezentuje graf č. 15.

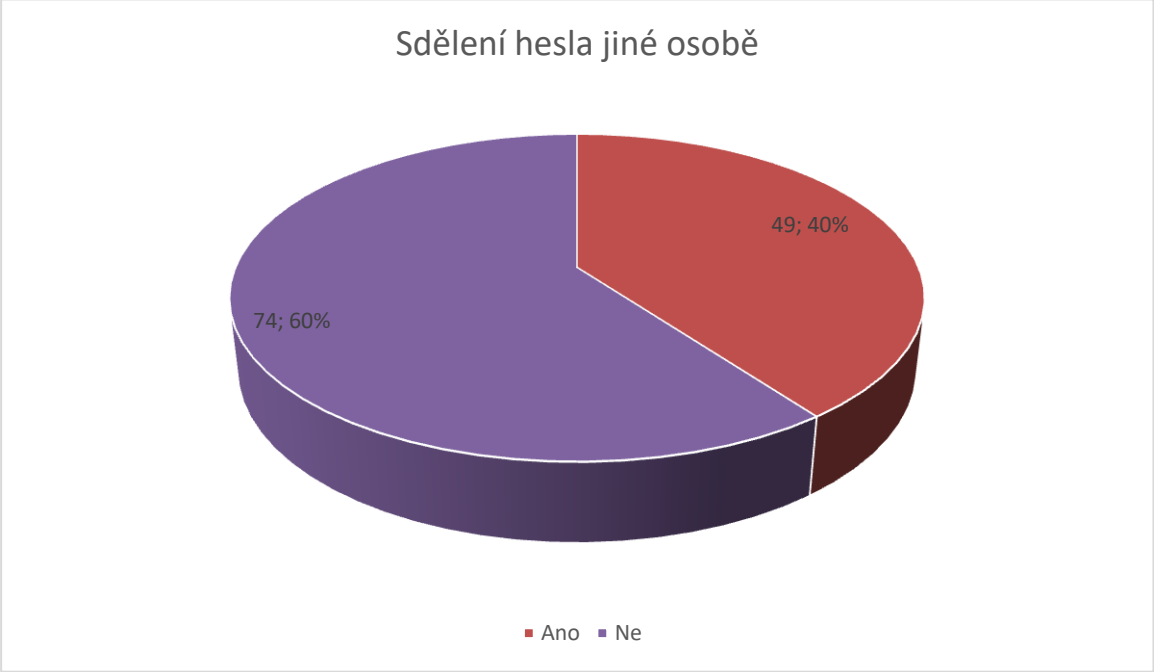
Graf č. 15: Napsané heslo

Zdroj: vlastní výzkum

Otázka č. 16: Sdělil/a jste někdy někomu své heslo k účtu na sociální síti?

Z odpovědí na tuto otázku je zřejmé, že 60 % (74) respondentů nikomu své heslo k účtu na sociální síti nesdělilo, nicméně celých 40 % (49) respondentů tak učinilo. Ačkoliv je tento výsledek lepší než výsledky předcházejících odpovědí, i zde je dostatek prostoru pro zlepšování a informování uživatelů sociálních sítí o rizicích. Výsledky jsou znázorněny v grafu č. 16.

Graf č. 16: Sdělení hesla jiné osobě



Zdroj: vlastní výzkum

Otázka č. 17: Přidal/a jste si na sociální síti někdy člověka, kterého osobně neznáte?

Z odpovědí na tuto otázku je patrné, že 68 % (84) respondentů si někdy na sociální síti přidalo do přátel osobu, kterou osobně neznají. Pouze 32 % (39) respondentů uvádělo opa, tedy, že si nikdy neznámého člověka do přátel nepřidali. Z uvedeného je zřejmé, že i zde se projevují významná bezpečnostní rizika, která si uživatelé patrně neuvědomují, popř. nepřipouštějí. Výsledky odpovědí na tuto otázku představuje graf č. 17.

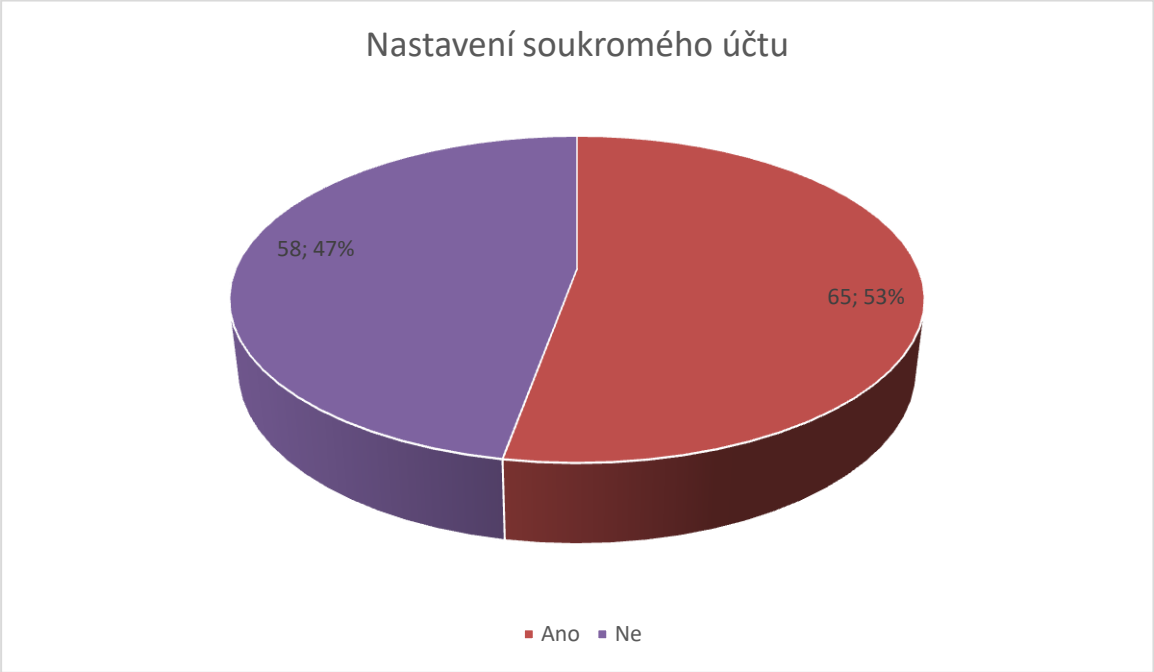
Graf č. 17: Přidání neznámé osoby do přátel

Zdroj: vlastní výzkum

Otázka č. 18: Máte účet nastaven tak, aby bylo co nejméně osobních údajů přístupno veřejnosti (jako soukromý, více informací se zobrazuje přátelům, popř. osobám, jimž sledování povolíte)?

Osmnáctá otázka zjišťovala, jak mají respondenti nastavené soukromí a zda údaje sdílejí spíše jen s okruhem svých známých nebo s kýmkoliv, kdo na jejich profil přijde. Z odpovědí respondentů bylo patrné, že 53 % (65) respondentů mělo účet z hlediska soukromí nastavený tak, aby řada osobních údajů byla k dispozici jen přátelům, nicméně zbývajících 47 % (58) respondentů toto nastavení soukromí nemělo. Výsledky odpovědí na tuto otázku představuje graf č. 18.

Graf č. 18: Nastavení soukromého účtu

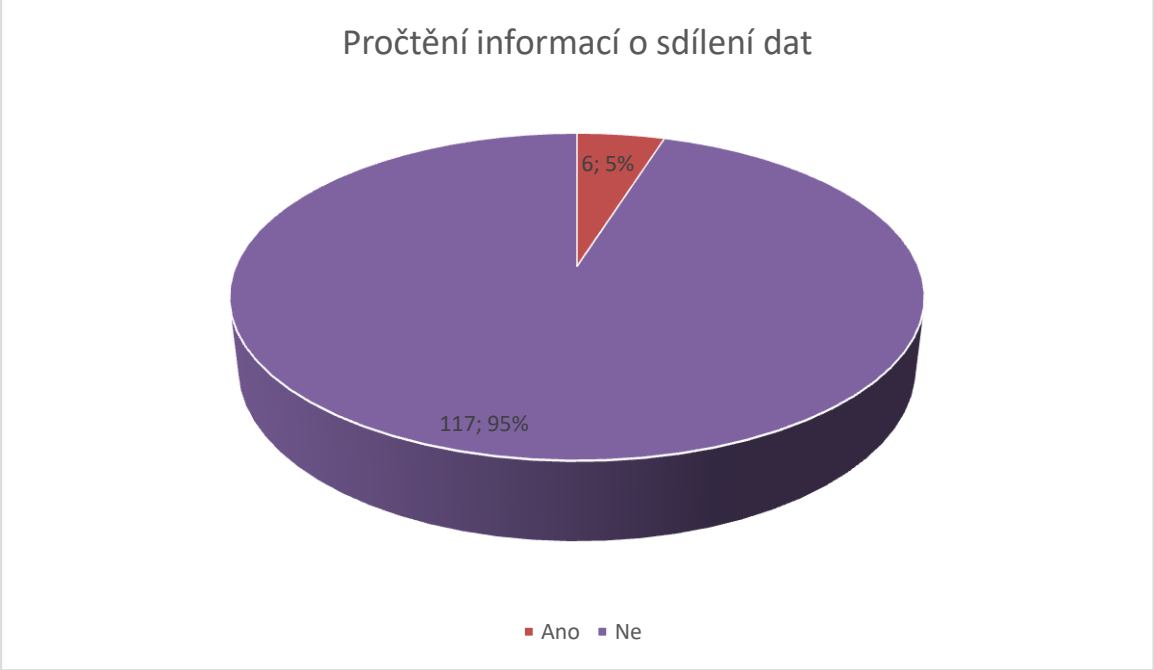


Zdroj: vlastní výzkum

Otázka č. 19: Pokud nějaká aplikace vyžaduje souhlas s tím, že získá přístup k některým Vašim údajům (např. jménu, e-mailu, seznamu přátel apod.) věnujete pozornost přečtení všech podmínek a možnosti souhlas v budoucnu odvolat?

Devatenáctá otázka v dotazníku se zaměřovala na další aspekty ochrany soukromí a osobních údajů, které má jedinec uvedeny na profilu na sociální síti, a to na jejich sdílení s aplikacemi, které to často výměnou za nějakou formu „protislužby“ od uživatele sociální sítě vyžadují. Jak vyplynulo z odpovědí respondentů, je zřejmé, že naprostá většina uživatelů sociálních sítí ve skutečnosti informace o tom, jaké údaje budou sdíleny, za jakým účelem, jak lze souhlas odvolat apod. vůbec nečte, což je zásadním negativem a z bezpečnostního hlediska také rizikem. 95 % (117) respondentů totiž pročtení těchto informací dostatečnou pozornost nevěnuje, jen 5 % (6) respondentů uvedlo opak, tedy, že si tyto informace čtou. Výsledky odpovědí na tuto otázku znázorňuje graf č. 19.

Graf č. 19: Pročtení informací o sdílení osobních dat s aplikací



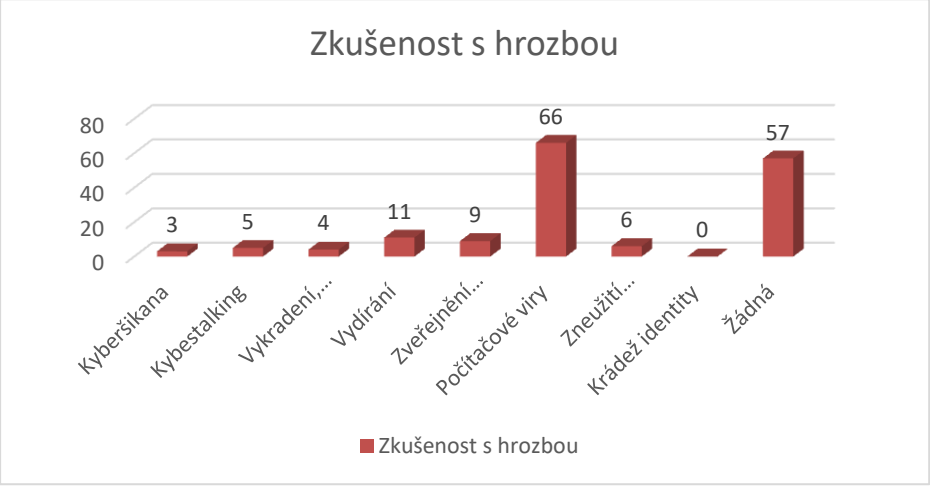
Zdroj: vlastní výzkum

Otázka č. 20: Setkal/a jste Vy osobně se někdy s některým z následujících negativních jevů spojených s užíváním sociálních sítí?

Poslední otázka v dotazníkovém šetření pak zjišťovala, zda mají respondenti osobní zkušenost s některými hrozbami, které jsou s užíváním sociálních sítí poměrně často spojeny. V této otázce mohli respondenti opět volit i více než jednu odpověď, aby se podařilo postihnout problematiku v celé její šíři (vycházelo se z toho, že někteří respondenti mohou mít zkušenost i s více hrozbami). Proto je také odpověď na tuto otázku vyhodnocena sloupcovým grafem a v absolutních číslech.

Z odpovědí respondentů vyplynulo, že úplně nejčastěji měli respondenti zkušenost s počítačovým virem, který infikoval jejich počítač v souvislosti s používáním sociálních sítí. Tuto možnost zvolilo 66 respondentů. Druhou nejčastější odpovědí bylo, že respondent s žádnou hrozbou z uvedených zkušenost neměl, tuto variantu uvádělo 57 respondentů. Ostatní hrozby se sice vyskytovaly výrazně méně často, nicméně až na krádež identity, kterou neuvedl žádný respondent, se s nimi respondenti alespoň ojediněle setkali. 11 respondentů mělo zkušenost s vydíráním, 9 se zveřejněním intimních informací, popř. fotografií, 6 se setkalo se zneužitím osobních údajů, 5 mělo zkušenost s kyberstalkingem, 4 měly zkušenost s trestnými činy jako bylo například vykradení či podvod v návaznosti na informace čerpané z profilu na sociálních sítích, 3 respondenti se pak setkali s kyberšikanou. Výsledky jsou komplexně znázorněny prostřednictvím grafu č. 20.

Graf č. 20: Zkušenost s některou s bezpečnostních hrozeb na sociálních sítích



Zdroj: vlastní výzkum

5 ZHODNOCENÍ A DOPORUČENÍ

V této kapitole práce jsou nejprve shrnuty a dány do vzájemného kontextu výsledky výzkumu, které byly výše představeny (včetně toho, že jsou některé údaje dány do kontextu s charakteristikami výzkumného souboru), dále jsou také formulována doporučení pro praxi (tj. vlastní návrhy) a konečně je také zhodnoceno naplnění cílů výzkumu, které byly formulovány na počátku studie.

5.1 Shrnutí výsledků

Ze zjištěných údajů vyplynulo, že ve výzkumném souboru převažovaly spíše ženy, a to mladšího věku, nejpočetnější byla skupina ve věku 21-25 let, druhá nejpočetnější pak skupina ve věku 18-20 let, přičemž více než polovina respondentů žila v hlavním městě Praze, zbytek ve Středočeském kraji. Převažovali respondenti se středoškolským vzděláním, nicméně ve výzkumném souboru bylo i s ohledem na věk poměrně mnoho studentů, tj. jejich vzdělání ještě nebylo ukončeno a je zde předpoklad, že se bude dále zvyšovat. Lze tedy říci, že respondenti byli poměrně typičtí mladí lidé dnešní doby, kteří jak se ukázalo měli se sociálními síti až na jednu výjimku všichni zkušenosti a 98 % respondentů sociální sítě aktivně využívalo v současné době., čímž byl výzkumný soubor dobře zvolen i z toho hlediska, že naprostá většina účastníků mohla poskytnout i data týkající se vlastního zabezpečení jejich účtu na sociální síti, což byly údaje pro tento výzkum stěžejní. Nejčastěji respondenti využívali sociální sítě Facebook a Instagram, ostatní sociální sítě byly využívány výrazně méně. Zde je zajímavé, že zatímco v případě Facebooku nebyly zjištěny zásadní rozdíly mezi pohlavími, Instagram výrazně častěji využívaly ženy (ve 46 z 52 případů). Třetí nejvyužívanější sítí byl LinkedIn, který využívali jak muži, tak ženy a převažovaly zde již starší respondenti v rámci zkoumané kategorie, tj. lidé ve věku 31-35 let, popř. i lidé ve věku 26-30 let. Respondenti nejčastěji využívaly 1-2 sítě, více sítí obvykle využívaly ženy, a to zejména mladší ženy ve věku do 25 let.

Pokud se týká účelu využívání sociálních sítí, nejčastěji respondenti všech věkových kategorií i obou pohlaví využívají sociální sítě za účelem kontaktu s přáteli. Dále jsou však sociální sítě oběma pohlaví poměrně často využívány rovněž za účelem seznámení se s novými lidmi, což může být základem pro bezpečnostní rizik. Třetím nejčastěji uváděným důvodem, který uváděli především ženy, bylo sledování oblíbených značek produktů.

Z hlediska bezpečnosti sice 80 % respondentů deklarovalo, že je pro ně bezpečnost na sociálních sítích důležitá, nicméně z odpovědí na další otázky leckdy vyplývalo, že jí nevěnují dostatek pozornosti, popř. v řadě oblastí nedbají doporučení a zásad bezpečného používání sociálních sítí (nezávisle na tom, zda proto, že zásady neznají nebo proto, že jim nevěnují pozornost, popř. je podceňují, což již nebylo předmětem zkoumání). Z výzkumu však vzešlo, že se sice většina respondentů přihlašuje na sociální sítě ze svého zařízení (mobilního telefonu či tabletu, popř. počítače), nicméně i tak je poměrně rizikovým faktorem, že 79 % respondentů si ukládá hesla, 83 % respondentů nemá bezpečné heslo a 89 % respondentů má heslo někde napsané, kde se k němu však může za určitých okolností dostat i jiná osoba. Zde je nutné zmínit, ž e se nepodařilo identifikovat rozdíly v souvislosti s charakteristikami výzkumného souboru jako je věk, pohlaví, vzdělání či místo bydliště.

Dalším rizikovým jednáním, které vede k nedostatečnému zabezpečení účtu bylo sdělení hesla jiné osobě, které připustilo 40 % respondentů a dále přidání si osoby, kterou jedinec osobně nezná. V tomto případě se z hlediska charakteristiky výzkumného souboru ukázalo, že častěji se těchto jednání dopouštějí ženy než muži. 47 % respondentů také nemá dostatečně chráněné osobní údaje prostřednictvím nastavení účtu jako soukromého, zde převažovali spíše mladší jedinci do 25 let, kteří tuto odpověď uváděli častěji než jedinci starší. Zásadním zjištěním pak bylo, že 95 % respondentů (nezávisle na charakteristikách výzkumného souboru tak činili skoro všichni respondenti) připustilo, že nečte informace o poskytnutí osobních údajů, které bývá často některými aplikacemi vyžadováno výměnou za nějakou protislužbu, kterou aplikace nabízí.

Navzdory skutečnosti, že zabezpečení uživatelského účtu na sociálních sítích u většiny uživatelů nebylo optimální, téměř polovina, tj. 46 % (57) uživatelů se zatím v této souvislosti nesetkalo s žádnou bezpečnostní hrozbou a nejčastější bezpečnostní hrozbou, kterou uvádělo 54 % (66) respondentů byl počítačový virus, ostatní bezpečnostní hrozby se sice vyskytovaly poměrně zřídka, nicméně vyskytovaly se, což s ohledem na fakt, že třeba vydírání či kyberstalking a kyberšikana naplňují skutkové podstaty závažných trestných činů stejně jako krádeže či loupeže, k nimž došlo v souvislosti s tím, že respondent uvedl informace, které pachatel následně zneužil na sociální síti, je poměrně závažným zjištěním, ze kterého je třeba vycházet při formulaci dalších doporučení. Zajímavé z hlediska charakteristiky výzkumného

souboru bylo rovněž zjištění, že například obětí kyberšikany, kyberstalkingu, případně zveřejnění intimních informací či fotek se stávali častěji ženy.

5. 2Formulace doporučení pro praxi

V návaznosti na zjištění realizovaného výzkumu, je nyní zapotřebí formulovat vlastní návrh řešení, který spočívá v doporučeních pro praxi. Především je nutné dnešní mladou generaci i ve školách důsledně vést k tomu, aby dodržovala zásady bezpečného používání sociálních sítí, poukázat na výhody sociálních sítí, ale i na jejich rizika. V mladém věku totiž lidé tyto informace mohou snadno vstřebat a již v počátcích svého působení na sociálních sítích aplikovat.

Stejně tak by bylo velmi vhodné, aby byly realizovány i kampaně pro dospělé, které by byly vysílány např. v televizi, dostupné na internetu, velmi dobré by bylo, pokud by se do těchto kampaní aktivně zapojily i samotné sociální sítě, které mají rovněž zájem na bezpečnosti svých uživatelů (například Facebook průběžně nějaké kroky v této oblasti podniká, je však otázkou, zda jsou dostačující). Je samozřejmě také žádoucí, aby i pracovníci například policejních orgánů byly řádně školeni za účelem vyšetřování a řešení kriminality spojené se sociálními sítěmi, velmi prospěšné by mohly být rovněž besedy s policisty, kteří by zejména rizikovým skupinám (senioři, mladí lidé apod.) poskytovali informace o všech rizicích spojených s používáním sociálních sítí, ale zároveň jim poskytli alternativu, jak je používat bezpečně. Cílem totiž rozhodně není odradit lidi od používání sociálních sítí, které v dnešní době nesporně plní řadu užitečných úkolů, ale je důležité je naučit, jak používat sociální sítě bezpečně.

Uživatelům sociálních sítí pak lze doporučit dodržovat základní zásady bezpečnosti používání sociálních sítí, které byly představeny v podkapitole č. 3.2.2., přičemž obecně je důležité mít vždy na paměti, že člověk musí být obezřetný, nesmí každému na sociální síti věřit. Je třeba si uvědomit, že internet je pro člověka, který nechce informace o sobě sdělit, zárukou určité anonymity, která může být zneužita k celé řadě nekalých cílů, popř. k trestné činnost. Je tudíž vždy vhodnější o sobě na sociálních sítích sdílet spíše méně než více, zejména pokud se jedná o veřejné profily, kde si informace může vyhledat zcela každý bez toho, aby se to uživatel sociální sítě alespoň dozvěděl.

5.3 Zhodnocení naplnění cílů

V návaznosti na zjištěné údaje je nutné nyní pojednat o naplnění stanovených cílů. Cílem práce bylo analyzovat možné způsoby současného zneužívání sociálních sítí, porovnáním bezpečnostních skandálů identifikovat nejčastější příčiny bezpečnostních hrozeb a navrhnout způsoby snížení jejich rizika. Jak se ukázalo, způsobů zneužívání je celá řada, v této práci bylo na základě východisek z literatury pojednáno především o kyberšikanu, kyberstalking, navázání kontaktu s rizikovým jedincem (osobou, která se např. snaží získat osobní informace za účelem jejich zneužití nebo třeba páchání trestné činnosti jako je např. podvod či krádež), počítačové viry, zneužití osobních údajů nebo také krádež identity. Jak vyplynulo z výzkumu, respondenti měli nejčastěji zkušenosti s počítačovými viry, naopak krádež identity se ve výzkumu nevyskytla ni jednou, nicméně v menším počtu případů se vyskytovaly ostatní hrozby, které je nutné vnímat jako závažné.

Zá zásadní příčinu bezpečnostních hrozeb lze v kontextu zjištěných informací označit nedodržování zásad bezpečného používání sociálních sítí (bezpečné heslo, neukládat hesla, nepsat si hesla, nesdělovat hesla jiným osobám, nepřidávat si do přátel jedince, které osobně člověk nezná, nedostatečné prostudování, jaké informace a za jakým účelem budou předány při využití určité aplikace apod.), což byly problémy, které respondenti připouštěli skutečně ve vysokém počtu případů. V návaznosti na tento fakt pak byla v předchozí podkapitole formulována rovněž doporučení pro praxi. Hlavní cíl práce se tak podařilo naplnit.

Dílčím cílem práce bylo vyvrátit či potvrdit předpoklad nízkého stupně zabezpečení přihlašovacích údajů uživatelských účtů na sociálních sítích. V návaznosti na závěry realizovaného průzkumu se tento předpoklad podařilo potvrdit, neboť většina respondentů v dotazníkovém šetření skutečně neměla účet příliš dobře zabezpečený, což potvrzuje zejména fakt, že 79 % respondentů si ukládá hesla, 83 % respondentů nemá bezpečné heslo a 89 % respondentů má heslo někde napsané, kde se k němu však může za určitých okolností dostat i jiná osoba, 40 % respondentů pak připustilo, že heslo někdy sdělilo jiné osobě a 47 % respondentů nemá optimálně chráněné osobní údaje na profilu prostřednictvím jejich nastavení tak, aby se zobrazovali jen kontaktům, které má respondent v přátelích.

6 ZÁVĚR

Tématem předkládaného textu byla bezpečnost sociálních sítí. Cílem textu bylo analyzovat možné způsoby současného zneužívání sociálních sítí, porovnáním bezpečnostních skandálů identifikovat nejčastější příčiny bezpečnostních hrozeb a navrhnout způsoby snížení jejich rizika. Tento cíl byl naplňován za pomocí literární rešerše, na ni navazující dotazníkové šetření, které bylo následně adekvátním způsobem vyhodnoceno za pomocí běžných výzkumných metod jako je analýza a dedukce. Podařilo se přitom zjistit, že s většinou nejčastěji v literatuře zmiňovaných bezpečnostních hrozeb mají respondenti z hl. m. Prahy a Středočeského kraje alespoň nějaké zkušenosti, ve výzkumu se nevyskytla pouze krádež identity, která bude patrně vykazovat nižší četnost, než řada dalších hrozeb. Nejčastěji se lidé setkávají s počítačovými viry, kterých je v dnešní době mnoho, nicméně na druhou stranu jde o hrozbu poměrně běžnou, které se dá prostřednictvím antivirů a neklikání na neznámé odkazy poměrně efektivně předcházet, popř. lze vir z počítače odstranit, musí se o něm ovšem vědět, což je zásadním problémem s viry spojeným, že uživatel o něm, dokud nedojde například k destrukci souborů v počítači, software nebo třeba k proniknutí k jeho bankovnímu účtu nemusí vůbec vědět. V menším počtu případů však bylo patrné, že se respondenti setkali i s kyberšikanou, kyberstalkingem, vydíráním nebo třeba trestnou činností, při níž pachatel vycházel z informací na sociálních sítích, popř. i se zneužitím osobních údajů.

Po provedení analýzy získaných dat lze konstatovat, že hlavní příčinou, proč dochází k realizaci bezpečnostních hrozeb na sociálních sítí, je fakt, že lidé nedodržují bezpečnostní zásady a nemají dostatečně zabezpečený účet (velká část respondentů si ukládala hesla do zařízení, odkud se přihlašují, neměla bezpečné heslo stejně jako heslo měla někde poznamenané, kde se k němu mohla dostat jiná osoba, vyskytly se i případy, kdy lidé jiné osobě své heslo sdělili apod.

V této souvislosti je tedy základním způsobem obrany před hrozbami spojenými s používáním sociálních síti a pro zajištění určité míry bezpečnosti na sociálních sítích především nutné, aby lidé tyto pravidla znali a také je dodržovali. K tomu je potřeba především dostatečná edukace a informovanost populace, do které by se měly zapojit jak nejrůznější neziskové organizace, tak školy, policejní orgány, ale i média a pochopitelně i samotné sociální sítě, v jejichž zájmu je rovněž to, aby byla sociální síť používána bezpečně.

7 Seznam použitých zdrojů

7.1 Bibliografie

BEDNÁŘ, Vojtěch. *Internetová publicistika*. Praha: Grada, 2011. Žurnalistika a komunikace. ISBN 8024734524.

BURIAN, Pavel. *Internet inteligentních aktivit*. Praha: Grada, 2014. Průvodce (Grada). ISBN 8024751372.

ČERNÁ, Alena a kol. *Kyberšikana: průvodce novým fenoménem*. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-210-6374-7.

DĚDIČEK, Dominik. *Facebook.* Brno: Computer Press, 2016. ISBN 978-80-251-3196-1.

DISMAN, Miroslav. *Jak se vyrábí sociologická znalost: příručka pro uživatele*. 4., nezměn. vyd. Praha: Karolinum, 2011. ISBN 978-80-246-1966-8.

HAVLÍČKOVÁ, Daniela. Metodika - Kompetence, Kvalita, Kvalifikace, (sebe)Koncepce. Praha: Národní institut pro další vzdělávání, 2015. ISBN 9788087449509.

HERODEK, Martin. *Tablet pro úplné začátečníky*. Brno: Computer Press, 2014. ISBN 978-80-251-4333-9.

KOPECKÝ, Kamil., KREJČÍ, Veronika. Rizika virtuální komunikace (příručka pro učitele a rodiče). Olomouc: NET university, 2010, ISBN 978-80-254-7866-0.

KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: Grada Publishing, 2015. Průvodce (Grada). ISBN 978-80-247-5453-6.

KRÁL, Mojmír a David KRÁL. *Komunikace na počítači pro seniory*. Praha: Grada, 2016. Průvodce (Grada). ISBN 978-80-247-5812-1.

MATTERN, Joanne. *Instagram*. Minneapolis, Minnesota: Checkerboard Library, an imprint of Abdo Publishing, [2017]. Social media sensations. ISBN 1680775758.

PEACOCK, Michael. *Programujeme vlastní sociální síť v PHP 5*. Brno: Computer Press, 2012. ISBN 978-80-251-3626-3.

POSPÍŠILOVÁ, Marie. *Facebooková (ne)závislost: identita, interakce a uživatelská kariéra na Facebooku*. Praha: Univerzita Karlova, nakladatelství Karolinum, 2016. ISBN 978-80-246-3306-0.

PROCHÁZKA, David. *První kroky s internetem*. 3., aktualiz. vyd. Praha: Grada, 2010. Snadno a rychle (Grada). ISBN 978-80-247-3255-8.

PUGNEROVÁ, Michaela a Jana KVINTOVÁ. *Přehled poruch psychického vývoje*. Praha: Grada, 2016. Psyché (Grada). ISBN 978-80-247-5452-9.
ŘÍČAN, Pavel a Pavlína JANOŠOVÁ. *Jak na šikanu*. Praha: Grada, 2010. Pro rodiče. ISBN 978-80-247-2991-6.
SEDLÁKOVÁ, Renáta. Výzkum médií: nejužívanější metody a techniky. Praha: Grada, 2014. Žurnalistika a komunikace. ISBN 978-80-247-3568-9.

SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-80-247-4644-9.
SVOBODA, Václav. *Public relations moderně a účinně*. 2., aktualiz. a dopl. vyd. Praha: Grada, 2009. ISBN 8024728664.
TING, I-Hsien., Hui-Ju. WU a Tien-Hwa. HO. *Mining and analyzing social networks*. Berlin: Springer-Verlag, c2010. Studies in computational intelligence, v. 288. ISBN 3642134211.

7.2. Internetové zdroje

1) ČÍŽEK, Jakub. Před pěti lety se zrodila síť Google+. Nikdy se nestala Facebookem, ale není to ani mrtvola – Živě.cz.– O počítačích, IT a internetu [online] 2016 [cit. 09.07.2018]. Dostupné z: https://www.zive.cz/clanky/pred-peti-lety-se-zrodila-sit-google-nikdy-se-nestala-facebookem-ale-neni-to-ani-mrtvola/sc-3-a-182963/default.aspx
2) Bezpečnostní rizika (Security Risks) - ManagementMania.com. [online]. Copyright © 2011 [cit. 09.07.2018]. Dostupné z: https://managementmania.com/cs/bezpecnostni-rizika
3) Bezpečný internet | Rady pro bezpečné používání sociálních sítí. Bezpečný internet | Rady pro bezpečnost na internetu [online]. Copyright © 2016 [cit. 09.07.2018] Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/socialni-site/rady.aspx
4) FACEBOOK: Co můžu udělat pro trvalé zabezpečení účtu? soukromí [online]. Copyright © 2018 [cit. 10.07.2018] Dostupné z: https://www.facebook.com/help/213481848684090
5) KASÍK, Pavel. NÁVOD: Kdo má přístup k vašemu Facebooku? Zalepte si díry v soukromí [online]. Copyright © 2018 [cit. 10.07.2018] Dostupné z: https://technet.idnes.cz/navod-facebook-pristup-soukromi-aplikace-smazat-facebookovy-ucet-1cm-/sw_internet.aspx?c=A180322_080848_sw_internet_pka

6) Viry, které se šíří po sociálních sítích - Vím, kam klikám. Vím, kam klikám [online]. Copyright © 2017 [cit. 17.07.2018]. Dostupné z: http://www.vimkamklikam.cz/bezpeci-deti/viry-ktere-se-siri-po-socialnich-sitich
7) Ztráta identity - Policie České republiky. Úvodní strana - Policie České republiky [online]. Copyright © 2018 Policie ČR, všechna práva vyhrazena [cit. 17.07.2018]. Dostupné z: http://www.policie.cz/clanek/ztrata-identity.aspx
8) Skandály Facebooku nekončí. Sdílel data s čínskými výrobci mobilů, jeden je bezpečnostní hrozbou pro USA - info.cz[online]. Copyright © 2018 [cit. 06.06.2018] Dostupné z: https://www.info.cz/strategie/skandaly-facebooku-nekonci-sdilel-data-s-cinskymi-vyrobci-mobilu-jeden-je-bezpecnostni-hrozbou-pro-usa-31664.html
9) Co je GDPR - gdpr.cz[online] Dostupné z: https://www.gdpr.cz/gdpr/

8. Příloha č. 1 - Dotazník

Dotazník se zaměřuje na výzkum bezpečnosti a chování uživatelů na sociálních sítích. Dotazník je určen pro respondenty ve věku 18-35 let, kteří žijí v Praze, popř. ve Středočeském kraji. Pokud tyto podmínky splňujete, klikněte na „ano“ a budete přesměrováni k dotazníku. V opačném případě klikněte na „ne.“

1. Jste:
    a) Muž
    b) Žena
2. Kolik je Vám let?
    a) 18-20 let
    b) 21-25 let
    c) 26-30 let
    d) 31-35 let
3. Jaké je Vaše nejvyšší dosažené vzdělání?
    a) Základní
    b) Vyučen/a
    c) Středoškolské s maturitou

Vyšší odborné

d)
e) Vysokoškolské

4. Kde žijete?
   a) Hl. m. Praha
   b) Středočeský kraj – město, vesnice do 10 000 obyvatel
   c) Středočeský kraj – město nad 10 000 obyvatel
5. Jaký je váš socio-ekonomický status?
   a) Student
   b) Zaměstnanec
   c) Podnikatel
   d) Nezaměstnaný
   e) MD/RD
   f) Jiné
6. Založil/a jste si někdy profil na některé ze sociálních sítí (byť třeba i jen na zkoušku, který třeba nyní ani nevyužíváte)?
   a) Ano
   b) Ne)
7. Využíváte v současné některou ze sociálních sítí?
   a) Ano
   b) ne
8. Kolik sociálních sítí v současnosti využíváte?
   a) 0
   b) 1
   c) 2
   d) 3
   e) 4
   f) 5 a více
9. Které z následujících sociálních sítí využíváte?
   a) Facebook
   b) Twitter
   c) LinkedIn
   d) Instagram

Google+

e)
f) Jiné
g) Žádné

10. Z jakých důvodů sociální sítě využíváte? (Pokud sociální sítě nevyužíváte, zvolte důvod(y), pro který byste je nejspíše využívat byli ochotni začít).
    a) Kontakt s přáteli
    b) Seznámení se s novými lidmi
    c) Hledání zaměstnání
    d) Sledování oblíbených značek
    e) Sledování událostí
    f) Jiné
11. Je pro Vás důležité, aby váš účet na sociálních sítích byl dostatečně zabezpečen?
    a) Ano
    b) Ne
12. Odkud se k sociální síti nejčastěji přihlašujete?
    a) Z vlastního počítače doma
    b) Z vlastního mobilního telefonu či tabletu
    c) Z práce/ze školy
    d) Ze zařízení přítele, kolegy
    e) Odjinud
13. Ukládáte si hesla k profilům na sociální sítě do počítače či jiného zařízení, odkud se k sociální síti pravidelně přihlašujete?
    a) Ano
    b) Ne
14. Máte nastavené bezpečné heslo splňující následující požadavky: alespoň osm znaků, kombinace malých a velkých písmen s čísly, popř. i dalšími znaky?
    a) Ano
    b) Ne
15. Máte své heslo napsané někde, kde by se k němu eventuálně mohl dostat jiný člověk (např. v diáři, u počítače, z druhé strany telefonu apod.).
    a) Ano
    b) Ne

16. Sdělil/a jste někdy někomu své heslo k účtu na sociální síti?
    a) Ano
    b) Ne
17. Přidal/a jste si na sociální síti někdy člověka, kterého osobně neznáte?
    a) Ano
    b) Ne
18. Máte účet nastaven tak, aby bylo co nejméně osobních údajů přístupno veřejnosti (jako soukromý, více informací se zobrazuje přátelům, popř. osobám, jimž sledování povolíte)?
    a) Ano
    b) Ne
19. Pokud nějaká aplikace vyžaduje souhlas s tím, že získá přístup k některým Vašim údajům (např. jménu, e-mailu, seznamu přátel apod.) věnujete pozornost přečtení všech podmínek a možnosti souhlas v budoucnu odvolat?
    a) Ano
    b) Ne
20. Setkal/a jste se Vy osobně někdy s některým z následujících negativních jevů spojených s užíváním sociálních sítí?
    a) Kyberšikana
    b) Kybestalking
    c) Vykradení, podvod v důsledku informací ze sociální sítě
    d) Vydírání
    e) Zveřejnění intimních informací, fotek
    f) Počítačové viry
    g) Zneužití osobních údajů
    h) Krádež identity
    i) Žádná