Rizika na internetových sociálních sítích

Šárka Buberová

Bakalářská práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2014/2015

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Šárka Buberová**
Osobní číslo:	**L12403**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**kombinovaná**
Téma práce:	**Rizika na internetových sociálních sítích**

Zásady pro vypracování:

1. **Seznamte se s teoretickými základy problematiky sociálních sítí a rizik spojených s jejich využívámím.**
2. **Vymezte hlavní rizika spojená s využívámím sociálních sítí.**
3. **Připravte a realizujte veřejný průzkum v oblasti využití sociálních sítí a souvisejícími riziky.**
4. **Proveďte vyhodnocení průzkumu a porovnejte jej s předpokládanými riziky.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

[1] ECKEROVÁ, Lenka a Daniel DOČEKAL. Bezpečnost dětí na Internetu. Vyd. 1. Brno: Computer Press, 2013, 224 s. ISBN 978-80-251-3804-5.

[2] JIROVSKÝ, Václav. Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Vyd. 1. Praha: Grada, 2007. 288 s. ISBN 978-80-247-1561-2.

[3] PAVLIČEK, Antonín. Nová média a sociální sítě. Vyd. Praha:Oeconomica, 2010, 181 s. ISBN 978-80-245-1742-1.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Jakub Rak**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **6. února 2015**

Termín odevzdání bakalářské práce: **16. května 2015**

V Uherském Hradišti dne 20. února 2015

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení

doc. RNDr. Jiří Dostál, CSc.
děkan

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

V Uherském Hradišti 11. 04. 2015

.....
podpis studenta

ABSTRAKT

Bakalářská práce se zabývá analýzou rizika sociálních sítí na Internetu, popisuje možné zneužití, a minimalizování rizik pro uživatele. Vychází převážně z běžně dostupných materiálů. V teoretické části se práce věnuje historií vzniku a vývoji internetu a sociálních sítí.

V praktické části je popsán výzkum, který byl realizován pomocí anonymního dotazníku formou kvantitativního šetření.

Jeho hlavním cílem bylo zjistit, jaké jsou zkušenosti uživatelů s Internetem a povědomí o možných rizicích, která jsou spojena s jeho používáním.

Klíčová slova: Internet, sociální síť, kvantitativní šetření, sociálně patologické jevy, kyberkriminalita

ABSTRACT

The bachelor thesis analyzes the risks of social networks on the Internet, describes their possible misuse and minimization of the risks for users. It is largely based on commonly available materials. The theoretical part of the thesis deals with the history of the origin and development of the Internet and social networks.

The practical part describes the research, which was conducted using anonymous questionnaire in the form of quantitative survey.

Its main objective was to find out what the user experiences with the Internet are and awareness of the possible risks that are associated with its use.

Keywords: the Internet, Social Network, quantitative survey, socially pathological phenomena, cybercrime

Ráda bych poděkovala vedoucímu mé bakalářské práce Ing. Jakubu Rakovi za jeho ochotu, cenné rady, odborné vedení a čas, který mě věnoval.

Velké poděkování patří i mé rodině za trpělivost a podporu, kterou mně projevovala během zpracování bakalářské práce a během celého studia.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Žijeme v čase rychlých informací, bleskových vztahů, usnadněné a neosobní komunikace. Na tom má velkou „zásluhu“ Internet, který je fenoménem posledního čtvrtstoletí. Internet je již běžnou součástí našeho života, který nás ovlivňuje. Sociální sítě se na Internetu staly novým komunikačním kanálem, jsou a patří v současnosti k jedné z nejpoužívanějších částí webu. Pomocí sociálních sítí se prostřednictvím Internetu sdružují lidé, kteří by se jinak fyzicky nemohli setkat. V současné době prožívají sociální sítě rychlý rozvoj. O popularitě sociálních sítí svědčí i fakt, že se do nich připojuje stále více uživatelů. Účel sociálních sítí se různí, některé slouží ke sdílení informací a k zábavě, jiné pomáhají hledat práci, případně sdružují etnika nebo umělce. Jako v každém společenském nebo sociálním prostředí i zde dochází k sociálně patologickým jevům, které postihují zejména děti a mohou ústit až v kriminální činy. Sociálně patologickým jevem se rozumí chování jedince, které je charakteristické nezdravým životním stylem, nedodržováním nebo porušováním sociálních norem, zákonů a předpisů, dále také chování a jednání, které vede k poškozování zdraví jedince a prostředí, ve kterém žije, což ve svém důsledku ústí v individuální, skupinové či celospolečenské poruchy. A právě základní prevenci těchto poruch se dotýká tato bakalářská práce. Zejména zmínka o snížení rizik jejich vzniku a důsledků by mohla být užitečná.

I. TEORETICKÁ ČÁST

1 INTERNET A SOCIÁLNÍ SÍTĚ

Obecně lze konstatovat, že takovou explozi a informační boom, jaký zažíváme nyní, umožnil právě internet. Skutečnosti a události, ať pozitivní nebo negativní, jsou během několika minut známy po celém světě. Je to dobře nebo špatně? Internet přispěl obrovskou mírou ke globalizaci světa. Internet vznikal již před delší dobou. Jeho vývoj byl záležitostí výzkumných pracovišť a univerzit. Podnětem k rozvoji a vzniku bylo vypuštění první sovětské umělé družice Země, Sputnik, v roce 1957.

1.1 Historie Internetu

Spojené státy založily výzkumnou agenturu ARPA (Advance Research Projects Agency), která měla za úkol vést výzkum pro ministerstvo obrany USA. Agentura chtěla přímé propojení počítačů mezi svými základnami a spolupracovníky. Počátkem sedmdesátých let se různá pracoviště a univerzity propojily sítí ARPAnet. Postupem času se síť začala rozšiřovat.

Potíže s propojením řešil protokol TCP/IP (Transmission Control Protocol/Internet Protocol).

V roce 1979 USA vytvořily síť Usenet, která sloužila k posílání elektronické pošty. Rok 1981 přinesl zrod univerzitní sítě Bitnet, jež propojovala počítače IBM.

Evropská verze Bitnetu EARN (European Academic and Research Network) byla vyvinuta v roce 1984.

Vylepšovaly se programy pro posílání elektronické pošty, vznikl „zavináč“ @. Tento znak **@** je symbolická zkratka pro anglickou předložku **at** s významem *u, při, na*. Symbol vznikl snad jako písařská ligatura z latinského *ad* obdobného významu jako anglické *at* (není to však potvrzeno a existují i alternativní hypotézy). Je znám rovněž pod názvem **salamander** (s výslovností *salamandr*). V roce 1984 byl zaveden systém doménových adres, internetové adresy (např. .com, .org) a množství kódů pro jednotlivé země a v e-mailové adrese odděluje jméno uživatele a jméno domény.

Koncem osmdesátých let vytvořili v NSF (National Science Foundation) pět výpočetních center, které využívali výzkumníci a univerzity. Zformovali síť, která umožňovala nejen

připojení dalších počítačů na centra, ale i vzájemné propojení. V roce 1986 byla stvořena nová síť NSFnet, která se stala základním prvkem Internetu.

ARPAnet ukončil svou činnost v roce 1990.

Internet do České republiky pronikl v listopadu 1991, ale až 13. února 1992 bylo připojeno České vysoké učení technické v Praze.

Nejvyhledávanější službou Internetu je www (World Wide Web), která uchovává informace efektivně, přehledně v podobě webových stránek. Vznikla v roce 1991 v laboratořích v CERNu (Evropská organizace pro nukleární výzkum). Konzultant Tim Berners-Lee vymyslel systém textů s odkazy. Word Wide Web je informační prostor, který umí vyhledat a získat informace pomocí protokolu HTTP (HyperText Transfer Protocol).

Pro získání informací z webu je nezbytný prohlížeč – Netscape - zkonstruován v roce 1994 v Californii. [10]

Historie Internetu je krátká, jeho šíření je rychlé.

Vyhledat informace na webu je jednoduchá, rychlá záležitost. Informace jsou dostupné, přehledné.

1.2 Internet

Jednoduše řečeno Internet tvoří celosvětovou počítačovou síť. Umožňuje každému počítači na planetě komunikovat s jiným počítačem. Aby Internet mohl fungovat, musíme se připojit. To znamená připojit svůj počítač k místu, kde je možný vstup do Internetu samotného. Možností je několik od telefonní linky až po bezdrátové spojení přes družici. Internet po připojení umožní získat velké množství informací. Hitem internetu se staly takzvané webové stránky a jejich prohlížení.

Webové stránky jsou uschovány na zvláštních místech, kterým se říká servery. K jejich používání je třeba znát adresu stánky, kterou napíšeme do vstupního pole programu, který se nazývá prohlížeč webových stránek nebo také browser.

Internet neslouží jen pro vyhledávání a prohlížení informací, ale i k přijímání a odesílání zpráv pomocí elektronické pošty. Systém elektronické pošty využívá nespočet lidí, umožňuje kontaktovat velmi rychle kohokoliv, kdo je do ní zapojen. [4]

1.3 Rizika Internetu

Počítačový vir je zlomyslný počítačový program, který vytvořil a poslal zlomyslný programátor. Nosičem počítačového viru může být každý soubor. Stačí, aby se k němu připojil kód viru. Nebezpečí může představovat například dokument z Wordu, mohou být nakaženy tzv. makroviry.

Viry se mohou samy množit kopírováním. Umějí načíst adresy z adresáře elektronické pošty a samy se rozeslat.

Co může virus způsobit? V nejhorším případě je schopný zcela zničit informace, které jsou uložené na disku počítače. Nejméně rizikové je pouhé prohlížení stránek Internetu.

Použitím antivirového programu můžeme eliminovat riziko napadení virem. Antivirový program hlídá neustále pohyby souboru na počítači, které se zdají být podezřelé a v případě, že odhadne možné nebezpečí, zakročí. Antivirové programy jsou propojeny s programy elektronické pošty, kterou kontrolují. Je nezbytné aplikovat programy z autorizovaných zdrojů. Program má kompletní dokumentaci, obsahuje certifikáty pravosti, kódová čísla, ochranné hologramy a jiné.

Pravidelně svá data zálohujte. [4]

1.4 Právní aspekty Internetu

Zneužívání osobních údajů je bezpečnostní riziko, kterým se uživatel sociální sítě vystavuje. Zákon č. 101/2000 Sb., o ochraně osobních údajů vymezuje práva každého na ochranu před neoprávněných zasahováním do soukromí práva a povinnosti při zpracování osobních údajů.

Osobní údaj je dle § 4 písm. a) zákona *„jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu“.* [11]

Podle definice je osobním údajem například:

- Jméno a příjmení
- Fakturační adresa
- Rodné číslo
- E-mailová adresa, která obsahuje jméno a příjmení
- Číslo sociálního zabezpečení, číslo pasu, atd.

Citlivé údaje je možné zpracovávat, jen s výslovným souhlasem konkrétní osoby. Jsou to informace, které se týkají zdravotního stavu, politických, filosofických, náboženských nebo odborových cílů. [8]

1.5 Sociální sítě

Sociální síť, anglicky social network, je propojená skupina lidí, kteří se mohou navzájem ovlivňovat, mohou to být příbuzní, kamarádi. Tvoří se na základě kolektivních zájmů, rodinných vazeb nebo z jiných důvodů, jako je např. politický, kulturní či ekonomický zájem. Sociální sítí se nazývá služba na internetu, která umožňuje registrovaným členům vytvářet si osobní nebo firemní veřejný nebo částečně veřejný profil, sdílet informace, fotografie, videa, provozovat „chat“, komunikovat spolu a mnoho dalších aktivit. Internetová diskusní fóra se někdy považují také za sociální síť, kde si uživatelé vyměňují poznatky a názory na různá témata například finanční poradenství, automobily, těhotenství apod. Tato komunikace na sociálních sítích může probíhat soukromně mezi dvěma uživateli nebo hromadně mezi uživatelem a skupinou s ním propojených dalších uživatelů. Nejznámější a největší sociální sítí je Facebook.com.

Uživatelé sociálních sítí jsou teenageři i dospělí uživatelé. [1]

1.6 Historie sociálních sítí

První sociální síť přišla v roce 1997. Byl to projekt Sixdegrees.com, který tenkrát poskytoval možnost udělat si profil a spojit se s přáteli. Tato služba svůj provoz skončila v roce 2001 a právě tyto funkce formulovaly základ, který sociální sítě mají společný. Podle svého zakladatele projekt nebyl moc úspěšný, protože předběhl svou dobu.

Nejznámější sociální sítě: Facebook, Google+, Myspace, Twitter, Linkedln.

České sociální sítě: Lidé.cz, Spolužáci.cz, Líbímseti.cz, SitIT.cz, SportCentral.cz, ČSFD.cz. [1]

1.7 Druhy sociálních sítí

Existuje mnoho sociálních sítí. Některé z nich se těší velké oblíbenosti a poskytují zajímavé funkce, které poskytují svým uživatelům.

Uživatel se nejprve zaregistruje na webu, obvykle musí odsouhlasit podmínky použití webu a jeho zásady ochrany osobních údajů. Podmínky užití obvykle určují odpovědnosti, pravomoci a jiné, zásady ochrany osobních údajů stanoví, jak se bude zacházet s daty uživatele. [7]

Příklady současných sociálních sítí:

1.7.1 Facebook

Facebook (www.facebook.com) vznikl původně jako systém pro studenty Harvardské univerzity, postupem času se rozšířil na všechny univerzity a nyní je přístupný každému. Facebook založil devatenáctiletý Mark Elliot Zuckerberg 4. února 2004 spolu se svými přáteli. Na světě žije přes sedm miliard lidí, z nichž dvě miliardy mají přístup k internetu z toho se k Facebooku připojuje polovina těchto uživatelů. [9]

Facebook 1. ledna 2015 upravil podmínky používání a každý, kdo chce Facebook používat se musí řídit těmito pravidly. Nové podmínky se od předešlých výrazně neliší. Stále platí, že myšlenky, fotky i videa nahraná na Facebook patří tomu, kdo je vytvořil. Facebook si pouze vyhrazuje právo s každým nahraným obsahem volně nakládat a nemusí za to uživatelům nic platit, a to po dobu trvání příspěvku nebo statusu, tedy než se rozhodne uživatel příspěvek nebo status smazat. Výjimka platí v případě, že příspěvek už někdo sdílel.

Při aktivaci profilu uživatelé o sobě Facebooku dávají základní data, to platí i pro komunikaci s přáteli formou zpráv, takzvaných lajků, sdílení či komentářů, záznamů pravidelných návštěv. Facebooková aplikace v mobilním zařízení, shromažďuje data o poloze samotného zařízení operátorovi, telefonním čísle, IP adrese nebo časovém pásmu. Hlavním cílem není sledování uživatele, ale přizpůsobení aplikace, nalezení chyb, další vývoj a zisk Facebooku. [13]

Mezi přístupné funkce Facebooku patří:

- profil, který lze upravovat,
- uživatelé mohou aktualizovat svůj stav,
- spojit se s jinými uživateli, připojí-li si je jako přátele,
- komentovat stavové informace o přátelích, uživatelé mohou vyznačit specifický stav, že se jim *líbí*,
- publikovat a sdílet fotografie,
- přátelé si mohou mezi svými profily posílat zprávy, uveřejňovat a sdílet události,
- mohou vytvářet skupiny zdůrazňující určité aktivity, zájmy a připojovat se k nim. [7]

1.7.2 LinkedIn

LinkedIn (www.lindedin.com) je sociální síť pro obchodní kontakty, spolužáky a kolegy, která primárně slouží ke styku obchodních partnerů. Vznikl v roce 2003. Uživatelé LinkedIn mohou:

- upravovat svůj profil
- spojit se s kolegy
- znázornit vzájemné vazby mezi uživateli,
- doporučit jiné uživatele s ohledem na zaměstnání,
- spojit Twitter se svým profilem,
- vyrobit a zobrazovat obchodní profily. [7]

1.7.3 MySpace

MySpace (www.myspace.com) byl konfigurován v roce 2003, sociální síť je populární mezi mladšími uživateli, zvláště nejrůznějšími hudebními skupinami, především díky možnosti detailní úpravy profilu s užitím kódu HTML a snadného vsunutí audia do profilů. Mezi dostupné funkce patří:

- upravitelné profily umožňující:
    - vkládat kód HTML – uživatelé mohou upravit vzhled, barvy, celkový dojem svého profilu,
    - vložení audia,
    - komentáře,
    - okamžité nálady uživatele.

- skupiny – malé podmnožiny uživatelů,
- MySpace TV – zveřejňování videa,
- sjednocení a rozvoj aplikací třetích stran pomocí aplikačního rozhraní,
- diskusní fóra,
- ankety, které umožňují získat názor uživatele. [7]

1.7.4 Twitter

Twitter (www.twitter.com) vznikl v roce 2006. Jde o sociální síť, jejíž základ tvoří krátké zprávy v délce maximálně 140 znaků. Přesto nabízí velkou škálu pozoruhodných funkcí:

- profily lze upravovat jak nastavením barev, tak i obrázku na pozadí,
- uživatelé mohou aktualizovat svůj stav, odpovídat na stavové aktualizace jiných uživatelů,
- stavovou aktualizaci jiného uživatele přeposlat pomocí funkce ReTweet.

Jednoduché používání a poměrně malé množství základních funkcí Twitter hodně proslavilo. [7]

1.8 Emailová komunikace

E-mail – elektronická pošta je nejvyužívanější spojení dnešního internetu. Umožňuje rychlou komunikaci na velké vzdálenosti a téměř zadarmo. Cena, kterou platíme za tuto službu je zneužití v podobě nevyžádané elektronické pošty – spamu.

Součástí zpráv mohou být i připojené soubory, přílohy. Před otevřením přijatých souborů, příloh je účelné je otestovat nejprve antivirovým programem. Program kontroluje příchozí zprávy a usiluje o zjištění podezřelého obsahu. [6]

1.9 Internetové bankovnictví

Internetové bankovnictví nebo také online banking, zprostředkovává kontakt klienta a banky nepřetržitě 24 hodin denně, 7 dní v týdnu, komunikaci s bankou a přístup k vybraným produktům a službám banky.

O poskytnutí služby může požádat majitel účtu a je poskytována na základě písemně uzavřené smlouvy mezi klientem a bankou, dále je podmíněna vedením běžného účtu u banky.

Služba je poskytována prostřednictvím datových a veřejných komunikačních linek. Banka neodpovídá za jejich zabezpečení, z tohoto důvodu nemůže ovlivnit, pokud klientovi vznikne škoda v důsledku zneužití přenášených zpráv.

Banka má kompetenci požadavky a platební transakce dokumentovat. Údaje o požadavcích jsou archivovány po určitou dobu v bance ve smyslu zákona č. 21/1992 Sb., o bankách v platném znění. [12]

1.10 Nákupy přes Internet

Internet se může jevit jako nákupní středisko ve Vašem obýváku. Stačí si vybrat některý internetový obchod, vybrat si zboží, objednat a nakonec zaplatit. Výhoda spočívá v tom, že se nemusí nikam jezdit, nakupovat můžeme kdykoliv a ušetříme čas. Ceny v internetových obchodech bývají nižší než ceny v kamenných obchodech.

Nákup na Internetu může mít i své nevýhody. Nemůžeme se na vybrané zboží podívat, jak vypadá doopravdy, nemůžeme si ho osahat, vyzkoušet. Zboží vidíme jen na fotografiích.

Nakupování přes Internet přináší i množství nebezpečí, kterých je vhodné se vyvarovat nebo to aspoň zkusit.

1.10.1 Slovníček užitečných termínů

Autorizace je proces, ve kterém potvrzujeme svoji identitu. Setkáváme se s ní na aukčních webech, zvláště tam, kde budeme chtít něco prodávat. Provozovatel chce ověřit (autorizovat) platnost údajů.

CVM (Card Verification Metod nebo CVV (Card Verification Value) je název pro tří- či čtyřmístný kód umístěný na zadní straně platební karty. Využívá se k dodatečnému zabezpečení online placení.

Platební brána je služba, která umožňuje placení platební kartou na Internetu.

E-shop (e-obchod) je zkratka pro „elektronický obchod“, je to prostor na Internetu, kde můžeme nakupovat zboží.

Elektronická peněženka je název pro platební systém, který pracuje tak, že si do něj uložíme peníze a poté z něj můžeme čerpat.

Elektronické aukce jsou speciální elektronické obchody, zboží je prodáváno aukčním způsobem, zájemci o zboží „přihazuji“ a postupně zvyšují cenu zboží.

V Česku se první internetové obchody objevily v roce 1996. [3]

V roce 2013 utratili Češi v e-shopech kolem 58 miliard korun. Nakupují hlavně proto, aby ušetřili čas, srovnávají ceny, a pro velký výběr zboží.

Největší český internetový obchod je Alza.cz. [14]

1.10.2 Nakupování na internetu v ČR

Rok od roku stoupá počet lidí, kteří na internetu nakupují. Podle Českého statistického úřadu (ČSÚ) v roce 2013 meziročně stoupl počet nakupujících přes internet o více než 300 tisíc na tři miliony osob. Velké oblibě se těší zejména u mladších a vzdělanějších Čechů, ale třeba také ve skupině žen na rodičovské dovolené. [14]

1.10.2.1 Nákupy na slevových serverech

Jsou více rizikové než nákupy v e-shopech? Je lepší nakupovat v těch největších, je to stejné jako u e-shopů. Dá se jim věřit. Přejí si zákazníky a pečují o ně. Nevýhodou slevových serverů je, že jsou jen zprostředkovateli, tedy si kupujeme službu od někoho dalšího.

1.10.3 Základní pravidla a obezřetnosti při internetovém nakupování

Rozhodující pro bezpečné nakupování na Internetu je vybrat si důvěryhodný e-shop. Nakupováním ve známých a zavedených obchodech je internetové nakupování bezpečné. To je základní pravidlo nakupování na Internetu. Co hrozí při opomenutí tohoto základního pravidla? Můžeme se potkat s množstvím nepříjemností:

Zneužití platební karty, pokud informace ze své platební karty zadáte někomu, jehož záměr je zneužití karty, v okamžiku vám z karty odcizí Vaše peníze.

PIN k vaší platební kartě se nikdy nezadává na Internetu.

Zneužití identity na internetovém obchodě pokud se někomu podaří zjistit vaše přihlašovací údaje do internetového obchodu, může si nějaké zboží objednat nebo zjistit si řadu informací.

Proto je dobré zachovávat některá základní pravidla, která mohou snížit rizika jako je například:

- nakupování v ověřených obchodech,
- kde si nejsme jisti, nikdy neplatit předem,
- vyzvednout si zboží osobně,
- prověřovat si prodejce,
- pozorné čtení obchodních podmínek,
- varovné příznaky podvodů – nízká cena, chybějící kontakty a další. [3]

1.11 Bezpečnostní riziko

Bezpečnost se začala řešit na přelomu osmdesátých a devadesátých let minulého století. Lidé, kteří vyvíjeli Internet, se na počátku koncentrovali na vývoj technologie. V osmdesátých letech začal kolovat celosvětovou sítí první počítačový virus, změnil celou filozofii a poskytl nový pohled na bezpečnost.

V současnosti média informují v kontextu s Internetem o případech zneužitých dětí, o podvodných službách, finančních podvodech, útocích hackerů. Spousta případů by se nestala, kdyby uživatelé Internetu odpovědně chránili sami sebe, včas a zřetelně poučili své děti.

1.12 Sociální sítě rozmach a nebezpečí

Budoucnost sociálních sítí je slibná. Její popularita stále stoupá nejen u teenagerů, ale i u dospělých osob. Každý den se na sociální sítě a online komunity, které tvoří důležité spojení 21. století připojuje milióny lidí, kteří mají k dispozici internetové připojení. Internet? Sociální sítě můžeme využít i pro komunikaci s potenciálními i se stávajícími zákazníky.

Jejich nesporné výhody jsou rychlost komunikace, rozsáhlý okruh návštěvníků.

Jako ve všem jsou zde i nevýhody: možná závislost na sociální síti, kybernetická kriminalita, kybernetické výpalné, šíření materiálů se závadným obsahem, zneužití internetových stránek a další kyberzločiny.

2 INFORMAČNÍ BEZPEČNOST A OCHRANA

ISO – International Organization for Standrdization je mezinárodní organizace, která se zaobírá tvorbou norem, sídlí v Ženevě a byla založena 23. února 1947.

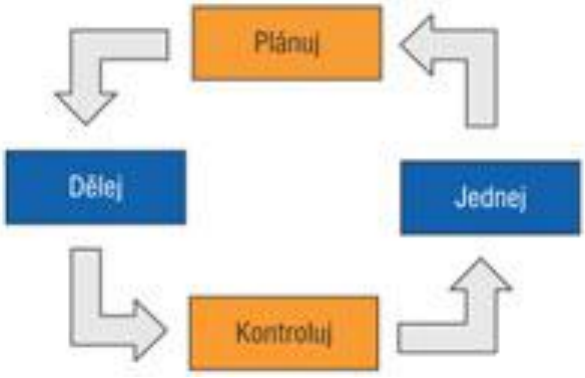
Pro Českou republiku je zastupující institucí Úřad pro technickou normalizaci, metrologii a státní zkušebnictví od roku 2009. [15]

V roce 2005 organizace ISO ohlásila zavedení nové řady norem ISO 27000, která řeší otázky řízení bezpečnosti informací. Vymezuje vztahy a hranice mezi existujícími a připravovanými bezpečnostními normami.

Hlavní složkou se stala mezinárodní norma ISO/IEC 27001:2005 – Systém řízení bezpečnosti informací, vychází z britského standardu BS 7799-2, která byla vydána v říjnu roku 2005 a jako ČSN v říjnu 2006.

Dnes se žádná instituce neobejde bez řízení bezpečnosti informací.

Systém řízení bezpečnosti informací je zaměřen na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu, zlepšování bezpečnosti informací. Také je založen na modelu PDCA – schematické vyjádření životního cyklu celého integrovaného systému řízení a současně zajišťuje tzv. zpětnou vazbu. [2]



Obr. 1 Princip Demingova PDCA modelu

2.1 Komu je norma ISO 27001 určena

Norma je určena pro organizace, které si chtějí své informace utřídit podle důležitosti, které by chtěly získat konkurenční výhodu, ale také chránit informační aktiva a minimalizovat ztráty způsobené jejich únikem. Také je určena pro osoby, které pracují s citlivými informacemi a osobními údaji.

Kriteriální norma ISO 27001 (celé označení ISO/IEC 27001:2005) vnáší pořádek do hodnot řízení, denní správy a provozu informačních systémů. Je to soubor opatření, metod, zásad a pravidel, vycházejících z osvědčených praktických postupů. Eliminuje slabiny a nabízí systematický, procesní a efektivní přístup k řízení bezpečnosti informací.

Eliminace rizik souvisí s možným narušením důvěrnosti a dostupnosti dat, sjednocuje postupy pro nakládání s informacemi, informační technologické procesy a odpovědnosti za bezpečnost pro celou firmu, zavádí správné pracovní návyky pro všechny zaměstnance týkající se bezpečnosti informací. Je to trvalý proces nezatěžující běžný provoz a zvyšující odpovědnost zaměstnanců za bezpečnost informací.

Proč společnosti zavádí normu ISO 27001? Protože je přínosná pro informační technologie, pro finance, pro marketing a naplňuje zákon na ochranu osobních údajů, zákon o elektronických komunikacích a autorský zákon. [17]

2.1.1 Výhody zavedeného systému

Výhodami systému jsou:

- soulad s legislativou ve smyslu zákonů 101/2000 Sb. Ochrana osobních údajů a trestní odpovědnost dle § 178 trestního zákoníku 140/1961 Sb. Neoprávněné nakládání s osobními údaji,
- vylepšení image organizace,
- větší důvěryhodnost pro zákazníka,
- posílení systému managementu organizace,
- pochopení slabých míst organizace z pohledu bezpečnosti informací, ideální rozložení nákladů na zvýšení bezpečnosti informací a jejich minimalizaci,
- systém zajistí rychlý přístup k informacím,
- zabrání nechtěné obměně informací, zneužití informací, ztrátu informací. [16]

2.2 Možnosti zneužití sociální sítě

S vývojem nových technologií se objevují i nové druhy trestné činnosti, kterým se společnost snaží zabránit. Může to být například kybernetická kriminalita, kyberšikana, kyberstalking, sexting, hacking, kybernetické výpalné, šíření materiálů se závadným obsahem, zneužití internetových stránek, spamming a další kyberzločiny.

2.2.1 Kybernetická kriminalita

Kybernalita je trestná činnost. Kybernetická kriminalita znamená jakýkoliv čin mířící k zneužití počítače nebo počítačového systému a informací, které jsou v něm uloženy. Jsou to zločinné aktivity za účelem krádeže, podvodu nebo padělání.

Rada Evropy počítačovou kriminalitu začala řešit koncem osmdesátých let. Podle studie vypracované v roce 1989 byla zveřejněna doporučení pro úpravy a tvoření nových zákonů. [5]

2.2.1.1 Klasifikace podle mezinárodní dohody o kyberzločinu

Tato dohoda je vytvořená pro řešení problémů spojených s mezinárodním charakterem počítačového zločinu a žádá, aby ty země, které podepsaly dohodu o kyberzločinu umožnily tuto trestnou činnost postihovat.

Dohoda dělí skutkovou podstatu podle obsahu:

- Zločiny proti důvěrnosti, integritě a dosažitelnosti počítačových dat a systémů, které se dále dělí na:
    - nezákonný přístup,
    - nezákonné odposlouchávání,
    - narušování dat,
    - narušování systémů,
    - zneužití prostředků.
- Zločiny se vztahem k počítači, které jsou děleny na:
    - počítačové padělání,
    - počítačový podvod.
- Zločiny se vztahem k obsahu počítače, především dětská pornografie.
- Zločiny se vztahem k autorským nebo obdobným právům. [5]

2.2.1.2 Klasifikace podle eEurope+

- zločiny porušující soukromí (ilegální sbírání, uchovávání, modifikace, zveřejňování a šíření osobních dat),
- zločiny se vztahem k obsahu počítače (pornografie, zvláště dětská, rasizmus, vyzývání k násilí, sebevraždám apod.),
- ekonomické (neautorizovaný přístup a sabotáž, hackerství, šíření virů, počítačová špionáž, počítačové padělání a podvody apod.),
- zločiny se vztahem k duševnímu vlastnictví (autorské právo apod.).

České orgány a Ministerstvo vnitra zpracovalo vlastní koncepci boje proti trestné činnosti v oblasti informačních technologií. Tuto koncepci doplnilo analýzou, která se zaměřuje více na oblast porušování autorských práv, nelegální kopírování a softwarové pirátství. [5]

2.2.1.3 Klasifikace kybernality z hlediska skutkových podstat

Základním ustanovením platného trestního zákona týkajícího se kybernality, je §257a „Poškození a zneužití záznamu na nosiči informací“- popisuje co není povoleno dělat s daty. Tento paragraf je jediným ustanovením, které je určeno pro informační technologie jako takové a postihuje vysoce kvalifikovanou trestnou činnost. Tento zákon se zaměřuje na tři formy činnosti:

- neoprávněné užití informací,
- zničení, poškození nebo učinění informací neupotřebitelnými,
- zásah do technického nebo programového vybavení počítače.

Mnoho dalších jednání lze postihnout samostatně, případně v rámci jednočinného souběhu s trestným činem podle § 257a. [5]

2.2.1.4 Kyberšikana

Kyberšikana je neustálé obtěžování jiné osoby s použitím internetu, mobilních telefonů či jiných informačních technologií.

Projevy kyberšikany:

1. Pomlouvání, urážení, posmívání nebo jiné ztrapňování za pomoci e-mailu, SMS zpráv.

2. Opatřování zvukových záznamů, videí, fotografií, které jsou upraveny a poté zveřejněny, aby oslabily osobu, která je obtěžována.
3. Tvorba internetových stránek, kde je urážena, pomlouvána daná osoba.
4. Zneužití cizího účtu – diskuzního, e-mailového apod.
5. Možné vydírání za pomoci telefonu či internetu.
6. Možné pronásledování či obtěžování za pomoci telefonu.

Cílem je někomu ublížit a ubližovat zejména společensky, fyzicky i psychicky. [19]

2.2.1.5 Kyberstalking

Kyberstalking je využití mobilních telefonů, internetu nebo jiných informačních a komunikačních technologií ke stalkingu.

Stalking znamená pronásledování, lov, opakované stupňované pronásledování, které může mýt rozmanitou podobu a intenzitu.

Projevy stalkingu:

1. Opakované i dlouhodobé pokusy kontaktovat oběť pomocí e-mailů, dopisů, SMS zpráv, telefonátů, posílání vzkazů na Skype apod.
2. Demonstrování moci a síly stalkera pomocí výhrůžek přímých i nepřímých, které budí v oběti strach a obavy.
3. Ničení majetku a věcí oběti například poškrábaní laku automobilu, rozbíjení oken, usmrcení domácího zvířete apod.
4. Stalker se sám vydává za oběť.
5. Snaha pošramotit reputaci oběti například rozšiřováním nepravdivých informací v okolí oběti.

Oběť a totožnost stalkera:

- Oběť stalkera osobně zná a ví, že ji pronásleduje.
- Oběť stalkera osobně zná a neví, že ji pronásleduje.
- Oběť stalkera nezná.

Kdo jsou stalkeři?

Může to být normální člověk, který je společenský, o kterém ani nejbližší okolí neví, že stíhá jinou osobu. Stalkeři bývají podle statistik většinou muži, komplikovanějšími útočníky jsou ženy pro svou systematičnost a cílevědomost.

Typologie stalkerů:

a) Uctívač
b) Poblouzněný milovník
c) Bývalý partner
d) Neobratný milovník
e) Sexuální útočník
f) Ublížený pronásledovatel
g) Kyberstalker

Následky kyberstalkingu jsou pro oběť stavy úzkosti, strachu, paniky, poruchy spánku, vzpomínky, které se neustále vrací. [20]

2.2.1.6 Sexting

Sexting česky sextování, je využívání informačních a komunikačních technologií dětmi a mladistvými. Slovo sexting je složenina ze slov sex a textování, což znamená elektronické rozesílání textových zpráv, fotografií nebo videa se sexuálním obsahem. Riziko spočívá ve zveřejnění fotografií nebo videa na internetu. Záminkou ke zveřejnění může být například ukončení vztahu mezi mladistvými. První případy sextingu se staly v roce 2005.

Sexting schvaluje šíření pornografie dětí a mladistvých, které je zakázáno celosvětově. V České republice jsou také zaznamenány případy sextingu, několik z nich se posuzují právě jako šíření dětské pornografie. Některé případy setingu mohou skončit i tragicky.

Z nedávné doby je známý případ Jessicy Logan (18) z USA, která spáchala sebevraždu, když její bývalý přítel zveřejnil její intimní fotografie, které mu sama poslala, když ještě spolu chodili. Jessica byla vystavena posměchu spolužáků, tlak neunesla a spáchala sebevraždu.

V České republice se případy sextingu řeší jednotlivě, některé případy jsou vyhodnoceny jako přestupky, jiné jako trestný čin, to záleží na typu fotografie a stylu opatření, u mladistvých osob může být sexting posuzován jako trestný čin ohrožování mravní výchovy mládeže, jiné případy sextingu se mohou vyřešit občansko-právní cestou. [21]

2.3 Soukromí uživatele, soukromí na sociálních sítích

Důležitý je zákon o ochraně osobních údajů č. 101/2000Sb. Osobní údaj je jakákoliv informace o fyzické osobě, která ji umožňuje identifikovat.

2.4 Minimalizace rizika

2.4.1 Některá doporučená pravidla při užívání sociálních sítích

Pro komunikaci na sociálních sítích se doporučuje dodržovat alespoň pár základních bezpečnostních pravidel, která mohou pomoct eliminovat riziko, nebo pomoci riziku se vyhnout.

- Pokud je to možné uvádějte o své osobě jen nezbytně nutné informace.
- Užívejte prověřený software s nainstalovaným antivirovým programem.
- Mezi své přátele si přidávejte osoby, které znáte.
- Na internet, sociální síť vstupujte pouze jen ze svého počítače.
- Nevyužívejte sociální sítě jako partnerskou seznamku.
- Užívejte bezpečnostní heslo o minimální délce 8 a více znaků v kombinaci velkých a malých písmen a dalších symbolů.
- Svůj profil si zabezpečte nastavením vyšší úrovně soukromí.
- Nahlaste zodpovědné osobě jakékoli porušení pravidel sociální sítě, obtěžování.

2.4.2 Projekty pro ochranu dětí a mládeže

Projekt E-Bezpečí

Projekt E-Bezpečí je celorepublikový projekt zaměřený na prevenci, vzdělávání, výzkum intervenci a osvětu spojenou rizikovým chováním na internetu a souvisejícími fenomény. Projekt je realizován Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého ve spolupráci s dalšími organizacemi.

Projekt se zaměřuje na nebezpečné internetové fenomény, které ohrožují jak děti, tak i dospělé uživatele internetu.

Projekt E-Bezpečí se specializuje zejména na:

- *kyberšikanu a sexting (různé formy vydírání, vyhrožování, poškozování obětí s pomocí informačních a komunikačních technologií),*
- *kybergrooming (komunikace s neznámými uživateli internetu vedoucí k osobní schůzce),*
- *kyberstalking a stalking (nebezpečné pronásledování s použitím ICT),*
- *rizika sociálních sítí (zejména Facebook),*
- *hoax a spam,*

- *zneužití osobních údajů v prostředí elektrotechnických médií.*

Obr. 2 Logo projektu E-Bezpečí

Základním východiskem činnosti projektu je terénní práce s nejrůznějšími cílovými skupinami, přednášková činnost, preventivní vzdělávací akce apod. Přednášky/besedy mapují jak konkrétní nebezpečné jevy, tak možnosti prevence a obrany proti útočníkům. Představa o problematice je vytvářena na základě modelových situací i skutečných kauz. Besedy jsou multimediální, jsou doprovázeny prezentací a videoukázkami.

Mezi cílové skupiny projektu E-Bezpečí patří žáci a studenti (od 1. Stupně ZŠ), učitelé, preventisté sociálně patologických jevů, metodici prevence, policisté (městská policie, Policie ČR), manažeři prevence kriminality, vychovatelé, pracovníci OSPOD a v neposlední řadě také rodiče.

Kromě vzdělávacích akcí realizuje projekt E-Bezpečí také pravidelná celorepubliková výzkumná šetření, zaměřená na rizikovou komunikaci v online prostředích, provozuje také online poradnu, vydává řadu zajímavých tiskovin pro žáky/učitele a realizuje řadu dalších aktivit. [18]

Existují další projekty, poradenská centra, které se věnují problematice spojené s využíváním internetu a internetových sociálních sítí dětmi. Jsou to například Linkabezpeci.cz, Bezpecnyinternet.cz, Internethotline.cz.

II. PRAKTICKÁ ČÁST

3 CÍL A METODOLOGIE BAKALÁŘSKÉ PRÁCE

Komunikace na Internetu je běžná součást našeho života. Stala se oblíbenou především díky sociálním sítím. Tato komunikace představuje určitá rizika nejen pro děti, ale také i pro dospělé.

3.1 Cíl bakalářské práce

Bakalářská práce si klade za cíl analyzovat bezpečnostní rizika sociálních sítí, popsat důsledky možného zneužití a navrhnout možná řešení, kterými by se měli uživatelé internetové sociální sítě řídit, aby minimalizovali tato rizika. Bezpečnostní rizika si uživatelé většinou sami neuvědomují. Sociální sítě jsou zpravidla určeny k seznámení a udržování vztahů se spolužáky, kamarády a dalšími osobami. Proto jsou oblíbeny hlavně u mladých lidí a právě oni jsou těmi, kdo na internetu zveřejňují osobní a soukromé informace. Při registraci na sociální síť jsou od uživatelů žádána různá data a údaje. Mezi takové údaje patří například jméno a příjmení, telefon, adresa bydliště a další osobní údaje. Proto před zaregistrováním na některou ze sociálních sítí je potřeba se přesvědčit, jak je v licenčních pravidlech popsáno nakládání s osobními údaji ze strany provozovatele. Obecně platí, čím méně toho o sobě vyplníme, tím méně se nám může stát.

3.2 Metodologie bakalářské práce

V bakalářské práci jsem aplikovala analýzu SWOT a dotazníkové šetření. Základním cílem SWOT analýzy bylo identifikovat klíčové trendy, vlivy a podmínky, které mohou působit na cílovou skupinu při užívání různých sociálních sítí. Tyto výsledky by měly pomoci omezit působení slabých stránek při používání internetových sociálních sítí, podpořit silné stránky, využít příležitosti a snažit se vyhnout případným hrozbám. Jako druhou metodu jsem zvolila dotazníkové šetření. Výzkum byl realizován pomocí anonymního dotazníku formou kvantitativního šetření. Jeho hlavním cílem bylo zjistit, jaké jsou zkušenosti uživatelů s Internetem a povědomí o možných rizicích, která jsou spojena s jeho používáním.

4 ANALÝZA SWOT

Analýza SWOT se používá pro klasifikování silných a slabých stránek společnosti, dále na příležitosti, které nám poskytuje současný stav, situace a nakonec se zaměřuje na hrozby, kterým můžeme vzdorovat. Prostřednictvím analýzy dokážeme najít problémy, lépe chápat souvislosti. Tato analýza se může využít i v jiných oblastech.

Analýza SWOT uvádí faktory, které působí nebo mohou působit při používání internetových sociálních sítí. Reciproční působení faktorů silných a slabých stránek na jedné straně proti příležitostem a hrozbám na druhé straně umožní najít nové hodnotné informace, jak je uvedeno v tabulce číslo 1.

Tab. 1 SWOT analýza

Silné stránky	**Slabé stránky**
▪ využití sociálních sítí k podnikání ▪ komunikace s přáteli, zákazníky ▪ sdílení příspěvků	▪ zveřejňování nepravdivých informací ▪ zveřejňování mnoho osobních údajů ▪ používání veřejné wifi sítě
Příležitosti	**Hrozby**
▪ soutěže, hry ▪ propagace značky, reklama ▪ získání nových kontaktů	▪ zpoplatnění služby ▪ zneužití účtu, krádež identity ▪ vydírání

[Zdroj: vlastní zpracování]

4.1 Vyhodnocení analýzy SWOT

V tabulce číslo 2 hodnotíme postupně jednotlivé parametry. U silných stránek a příležitostí použijeme kladnou stupnici od 1 do 5 s tím, že 5 znamená nejvyšší spokojenost a 1 nejnižší spokojenost. U slabých stránek a hrozeb použijeme zápornou stupnici od -1 do -5 s tím, že -5 znamená nejvyšší nespokojenost a -1 nejnižší nespokojenost.

Poté stanovíme jejich váhu, kdy váhou vyjádříme důležitost jednotlivých položek v dané kategorii – silné stránky, slabé stránky, příležitosti a hrozby. Váha se určí součtem vah

v dané kategorii a součet musí být roven 1. Čím vyšší číslo tím je větší důležitost položky v dané kategorii.

Dalším krokem stanovíme celkovou bilanci. Celkovou bilanci získáme tak, že vynásobíme hodnotu váhy s hodnocením, tyto hodnoty sečteme. Sečteme interní část SWOT analýzy - slabé a silné stránky, externí část SWOT analýzy – příležitosti a hrozby.

Posledním krokem vypočítáme konečnou bilanci tak, že odečteme interní část od externí části.

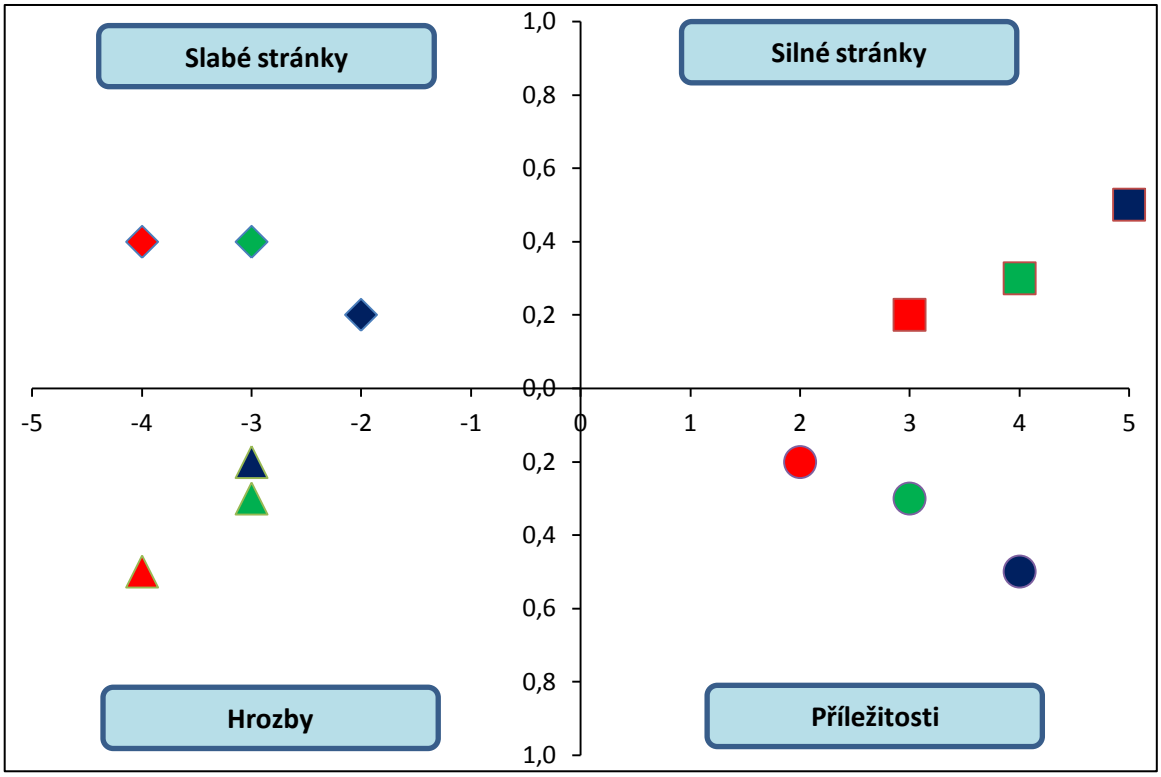
Tab. 2 Hodnocené parametry SWOT analýzy

Silné stránky	Váha	Hodnocení	Bilance
▪ využití sociálních sítí k podnikání	0,5	5	2,5
▪ komunikace s přáteli, zákazníky	0,3	4	1,2
▪ sdílení příspěvků	0,2	3	0,6
SOUČET	1	12	4,3
Slabé stránky	Váha	Hodnocení	Bilance
▪ zveřejňování nepravdivých informací	0,4	-3	-1,2
▪ zveřejňování mnoho osobních údajů	0,4	-4	-1,6
▪ používání veřejné wifi sítě	0,2	-2	-0,4
SOUČET	1	-9	-3,2
Příležitosti	Váha	Hodnocení	Bilance
▪ soutěže, hry	0,2	2	0,4
▪ propagace značky, reklama	0,3	3	0,9
▪ získání nových kontaktů	0,5	4	2
SOUČET	1	9	3,3
Hrozby	Váha	Hodnocení	Bilance
▪ zpoplatnění služby	0,2	-3	-0,6
▪ zneužití účtu, krádež identity	0,5	-4	-2
▪ vydírání	0,3	-3	-0,9
SOUČET	1	-10	-3,5

[Zdroj: vlastní zpracování]

Celková bilance:

- interní: 1,1
- externí: -0,2
- celkem: 0,9



Poznámka: Legenda

zveřejňování mnoho osobních údajů používání veřejné wifi sítě zveřejňování nepravdivých informací	sdílení příspěvků využití sociálních sítí k podnikání komunikace s přáteli, zákazníky
zneužití účtu, krádež identity zpoplatnění služby vydírání	soutěže, hry získání nových kontaktů propagace značky, reklama

Obr. 3 Grafické zobrazení SWOT analýzy [Zdroj: vlastní zpracování]

Záměrem SWOT analýzy bylo odhalit celkovou bilanci. Celková bilance SWOT analýzy internetových sociálních sítí je kladná, interní části mají převahu nad externími částmi. Z interní části je vidět, že silné stránky mají převahu nad slabými. Z externí části vidíme, že při používání internetových sociálních sítích je největší hrozbou zneužití účtu a krádež identity. Krádež identity je závažný problém. Před zneužitím osobních údajů je v první řadě dodržovat základní pravidla při práci na Internetu. Doporučení, jak se bránit odcizení identity jsou dostupné na různých internetových stránkách např. portál Ministerstva informatiky ČR.

4.2 Shrnutí SWOT analýzy

V tabulce číslo 2 jsme vyhodnotili postupně jednotlivé parametry.

Z analýzy jsme zjistili, že největší hrozba, která působí nebo může působit při používání internetových sociálních sítí je zneužití účtu a krádež identity, jako druhá velká hrozba, která působí nebo může působit na uživatele internetových sociálních sítí je vydírání a v poslední řadě nejméně závažnou hrozbou je zpoplatnění služby.

Ze slabých stránek SWOT analýzy, které působí nebo mohou působit při používání internetových sociálních sítí jsme zjistili, že největší slabinou, je zveřejňování mnoho osobních údajů, jako druhá velká slabina, která působí nebo může působit na uživatele internetových sociálních sítí je zveřejňování nepravdivých informací a v poslední řadě nejméně závažnou slabou stránkou je používání veřejné wifi sítě.

Největší příležitosti SWOT analýzy, které působí nebo mohou působit při používání internetových sociálních síti je získání nových kontaktů, jako druhá velká příležitost, která působí nebo může působit na uživatele internetových sociálních sítí je propagace značky, reklama a poslední příležitostí jsou soutěže a hry.

Provedenou analýzou bylo zjištěno, že nejsilnější stránkou, která působí nebo může působit při používání internetových sociálních sítí je využití sociálních sítí k podnikání, jako druhá silná stránka, která působí nebo může působit na uživatele internetových sociálních sítí je komunikace s přáteli, zákazníky a poslední silnou stránkou je sdílení informací.

5 DOTAZNÍKOVÉ ŠETŘENÍ

V praktické části bakalářské práce jsem použila kvantitativní metodu pomocí anonymního dotazníku. Cílem dotazníku bylo, získat informace o povědomí žáků střední školy o kyberprostoru. Dotazník obsahoval celkem 15 otázek, které směřovaly na zkušenosti s kyberprostorem, uživatelskou činnost a ochranu osobních dat. Dotazníky byly rozdány na střední škole Kostka ve Vsetíně, studentům 1. - 4. ročníku. Bohužel jsem neměla možnost se studenty spolupracovat, proto jsem dotazník svěřila předavateli, který na této škole studuje ve 4. ročníku. Informace o vyplnění dotazníku jsem poznamenala v úvodu, proto nebylo zapotřebí komentovat další sdělení.

Anonymní dotazník, který byl vytvořený pro bakalářskou práci obsahoval 15 otázek s možností odpovědi:

- ano/ne
- ano/ne/nepamatuji se
- výběr možností
- ano, vyjmenujte/ne.

Dotazníky jsem rozdala v celkovém počtu 100 kusů dotazníků s návratností 68%. Na dotazník odpovědělo celkem 68 studentů ve složení 15 (22,10%) mužů a 53 (77,90%) žen. Věk studentů byl v rozmezí 16 až 21 let. Studenti ve věku 16 let odpovídali v počtu 10 (14,70%) respondentů, studenti ve věku 17 let odpovídali v počtu 23 (33,83%) respondentů, studenti ve věku 18 let odpovídali v počtu 13 (19,12%) respondentů, studenti ve věku 19 let odpovídali v počtu 12 (17,64%) respondentů, studenti ve věku 20 let odpovídali v počtu 8 (11,77%) respondentů, studenti ve věku 21 let odpovídali v počtu 2 (2,94%) respondentů. Údaje, které jsem získala, následně vyhodnotila prostřednictvím tabulek a diagramového vyobrazení v Excelu, který jsem doplnila slovním popisem.

5.1 Vyhodnocení dotazníkového šetření

Otázka č. 1: **Máte doma počítač s připojením k internetu?**

Výsledky odpovědí v procentech jsou uvedeny v tabulce číslo 3 a diagramově vyobrazeny na obrázku číslo 4.

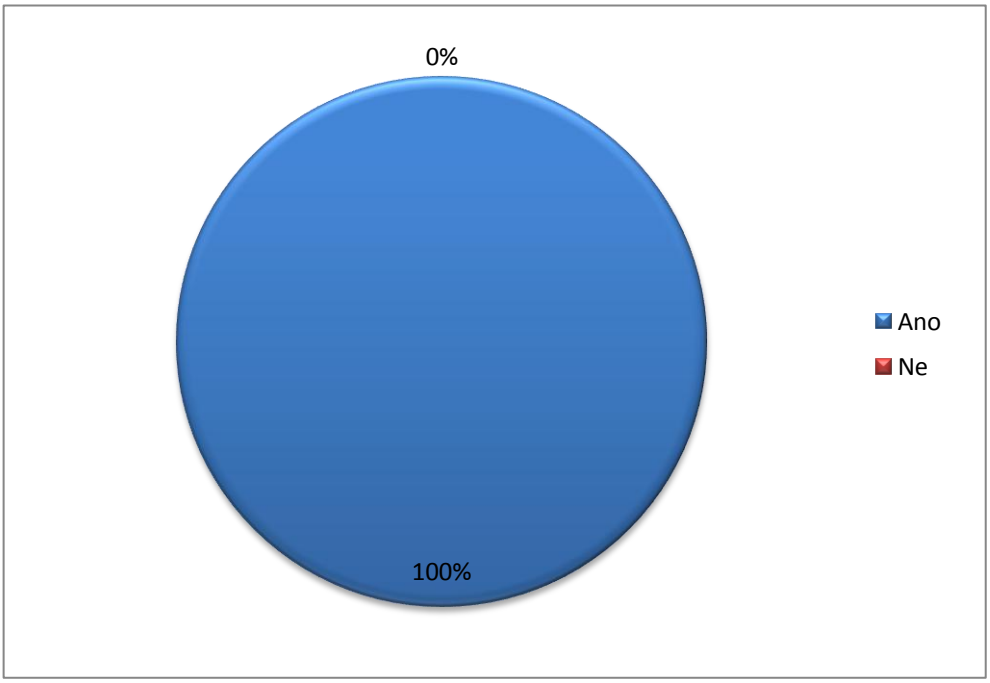
Možnosti výběru: Ano/Ne

Záměrem otázky bylo zjistit, zda studenti mají doma počítač s připojením k internetu.

Tab. 3 Domácí připojení k internetu

Možnost výběru	Počet odpovědí	Odpovědi v %
Ano	68	100%
Ne	0	0%

[Zdroj: vlastní zpracování]



Obr. 4 Diagramové znázornění otázky č. 1 [Zdroj: vlastní zpracování]

Otázka č. 2: **K jakému účelu počítač doma převážně využíváte?**

Výsledky odpovědí v procentech jsou uvedeny v tabulce číslo 4 a diagramově vyobrazeny na obrázku číslo 5.

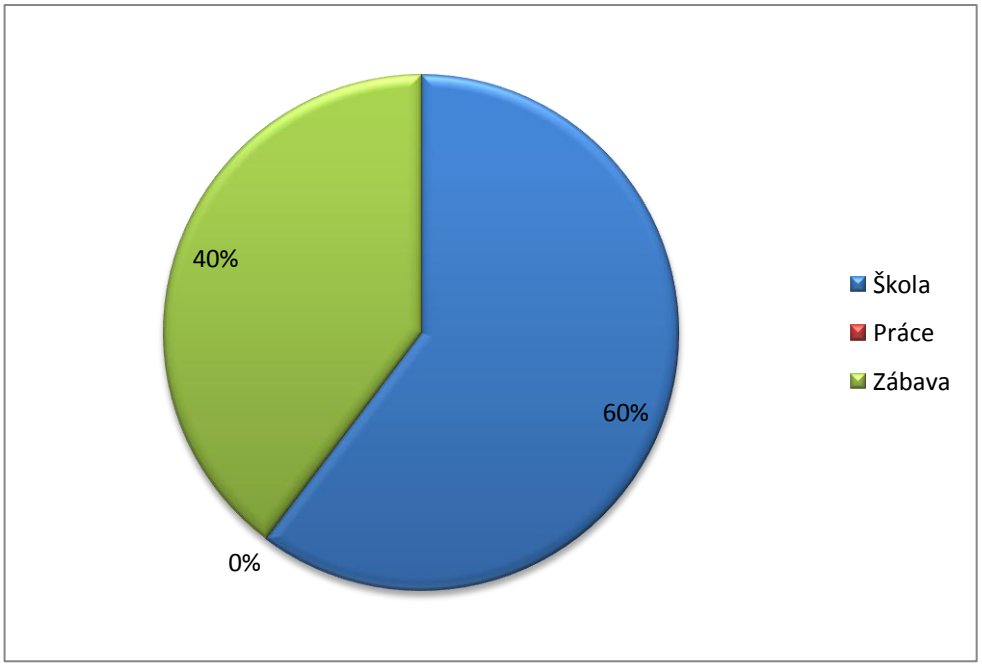
Možnosti výběru: 1 ze 3

Záměrem otázky bylo zjistit, k jakému účelu studenti převážně využívají domácí počítač.

Tab. 4 Účel využívání domácího počítače

Možnost výběru	Počet odpovědí	Odpovědi v %
Škola	41	60,30%
Práce	0	0%
Zábava	27	39,70%

[Zdroj: vlastní zpracování]



Obr. 5 Diagramové znázornění otázky č. 2 [Zdroj: vlastní zpracování]

Otázka č. 3: **Které nejznámější sociální sítě znáte?**

Výsledky odpovědí v procentech jsou uvedeny v tabulce číslo 5 a diagramově vyobrazeny na obrázku číslo 6.

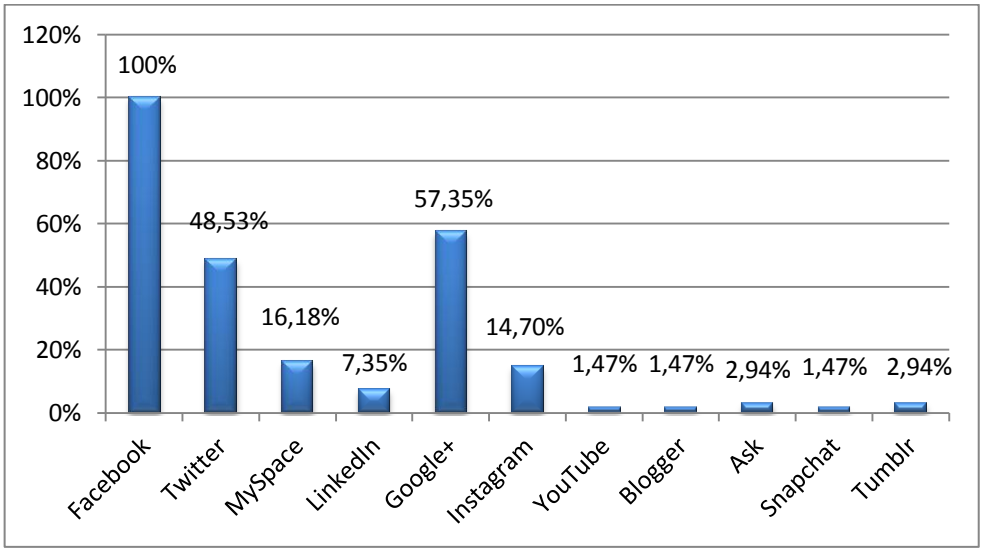
Možnosti výběru: 1 ze 6

Záměrem otázky bylo zjistit, které nejznámější sociální sítě studenti znají. Z výsledku je patrné, že pro studenty je nejvíce známou sociální sítí Facebook, Google+, Twitter.

Tab. 5 Znalost sociálních sítí

Možnost výběru	Počet odpovědí	Odpovědi v %
Facebook	68	100%
Twitter	33	48,53%
MySpace	11	16,18%
LinkedIn	5	7,35%
Google+	39	57,35%
Jiné: Instagram	10	14,70%
YouTube	1	1,47%
Blogger	1	1,47%
Ask	2	2,94%
Snapchat	1	1,47%
Tumblr	2	2,94%

[Zdroj: vlastní zpracování]



Obr. 6 Diagramové znázornění otázky č. 3 [Zdroj: vlastní zpracování]

Otázka č. 4: **Které české sociální sítě znáte?**

Výsledky odpovědí v procentech jsou uvedeny v tabulce číslo 6 a diagramově vyobrazeny na obrázku číslo 7.

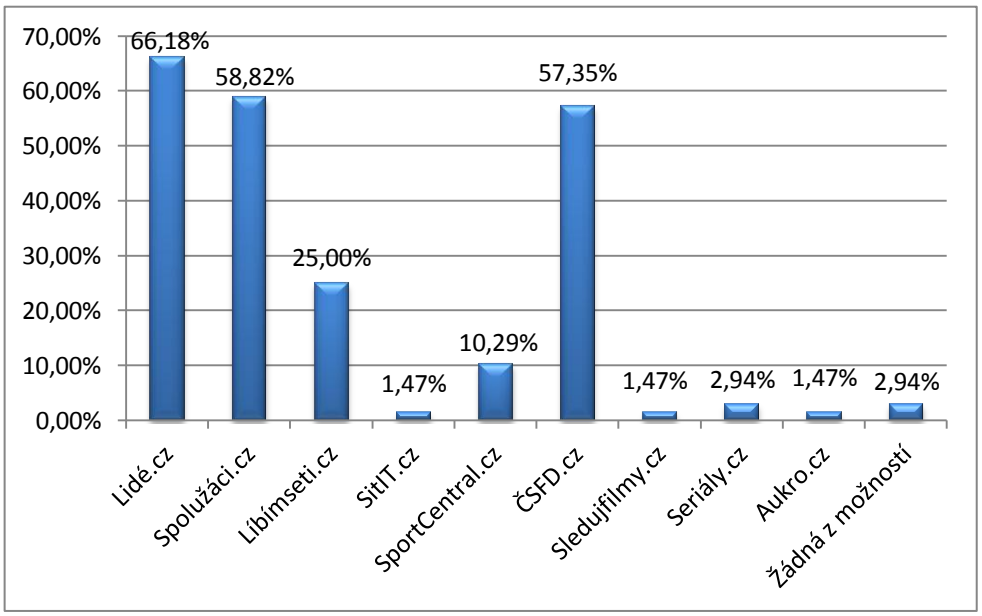
Možnosti výběru: 1 ze 7

Záměrem otázky bylo zjistit, které české sociální sítě studenti znají. Z výsledku je patrné, že pro studenty je nejvíce známou českou sociální sítí Lidé.cz, Spolužáci.cz, ČSFD.cz.

Tab. 6 Znalost českých sociálních sítí

Možnost výběru	Počet odpovědí	Odpovědi v %
Lidé.cz	45	66,18%
Spolužáci.cz	40	58,82%
Líbímseti.cz	17	25,00%
SitIT.cz	1	1,47%
SportCentral.cz	7	10,29%
ČSFD.cz	39	57,35%
Jiné: Sledujfilmy.cz	1	1,47%
Seriály.cz	2	2,94%
Aukro.cz	1	1,47%
Žádná z možností	2	2,94%

[Zdroj: vlastní zpracování]



Obr. 7 Diagramové znázornění otázky č. 4 [Zdroj: vlastní zpracování]

Otázka č. 5: **Kolik sociálních sítí využíváte?**

Výsledky odpovědí v procentech jsou uvedeny v tabulce číslo 7 a diagramově vyobrazeny na obrázku číslo 8.

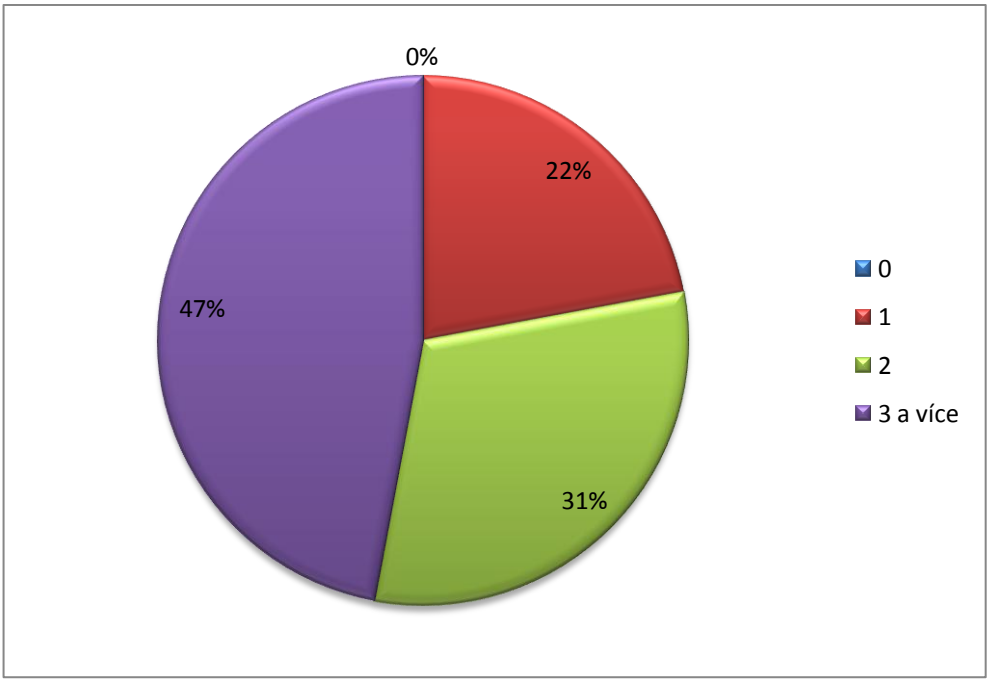
Možnosti výběru: 1 ze 4

Záměrem otázky bylo zjistit, kolik sociálních sítí studenti využívají.

Tab. 7 Využívání sociálních sítí

Možnost výběru	Počet odpovědí	Odpovědi v %
0	0	0%
1	15	22,05%
2	21	30,90%
3 a více	32	47,05%

[Zdroj: vlastní zpracování]



Obr. 8 Diagramové znázornění otázky č. 5 [Zdroj: vlastní zpracování]

Otázka č. 6: **Jak často navštěvujete Vaši sociální síť?**

Výsledky odpovědí v procentech jsou uvedeny v tabulce číslo 8 a diagramově vyobrazeny na obrázku číslo 9.

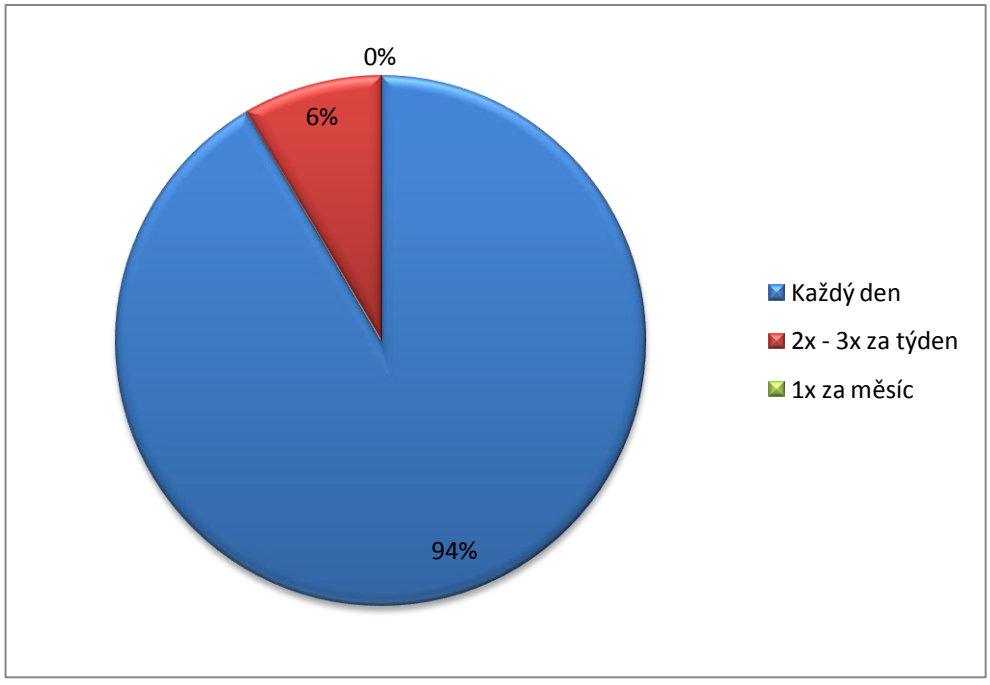
Možnosti výběru: 1 ze 3

Záměrem otázky bylo zjistit, jak často navštěvují studenti sociální síť.

Tab. 8 Návštěvnost sociální sítě

Možnost výběru	Počet odpovědí	Odpovědi v %
Každý den	64	94,12%
2x – 3x za týden	4	5,88%
1x za měsíc	0	0%

[Zdroj: vlastní zpracování]



Obr. 9 *Diagramové znázornění otázky č. 6 [Zdroj: vlastní zpracování]*

Otázka č. 7: **Prostudovali jste si důkladně podmínky registrace na sociální síti nebo změny podmínek po aktualizaci?**

Výsledky odpovědí v procentech jsou uvedeny v tabulce číslo 9 a diagramově vyobrazeny na obrázku číslo 10.

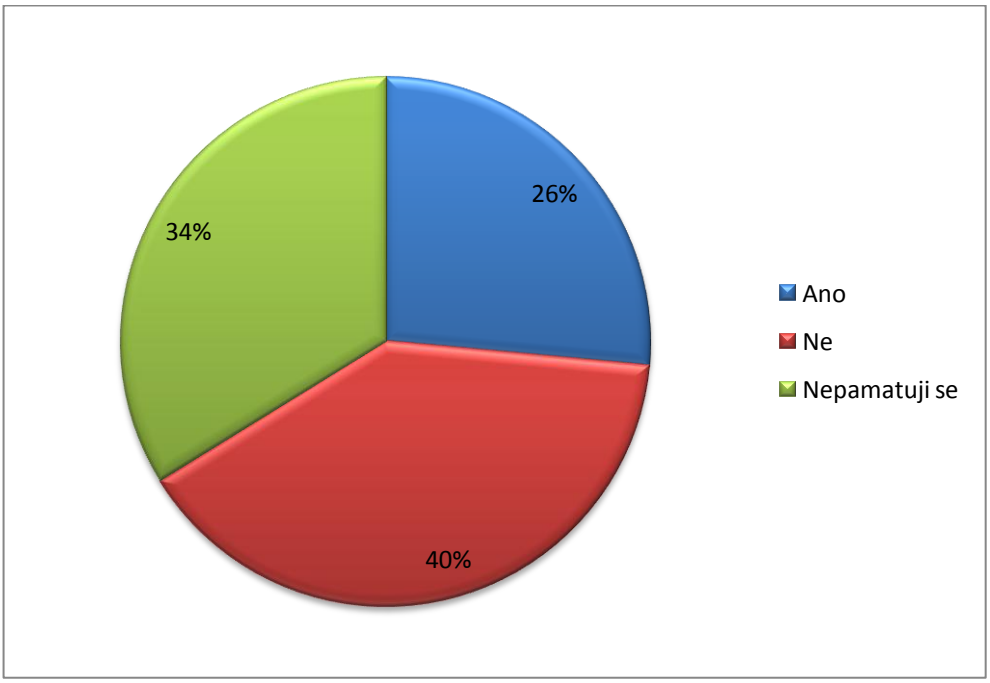
Možnosti výběru: 1 ze 3

Záměrem otázky bylo zjistit, zda si studenti důkladně prostudovali podmínky registrace na sociální síti nebo změny podmínek po aktualizaci.

Tab. 9 Prostudování podmínek registrace, změn po aktualizaci

Možnost výběru	Počet odpovědí	Odpovědi v %
Ano	18	26,47%
Ne	27	39,70%
Nepamatuji se	23	33,83%

[Zdroj: vlastní zpracování]



Obr. 10 Diagramové znázornění otázky č. 7 [Zdroj: vlastní zpracování]

Otázka č. 8: **Zrušili jste někdy registraci kvůli nevyhovujícím podmínkám?**

Výsledky odpovědí v procentech jsou uvedeny v tabulce číslo 10 a diagramově vyobrazeny na obrázku číslo 11.

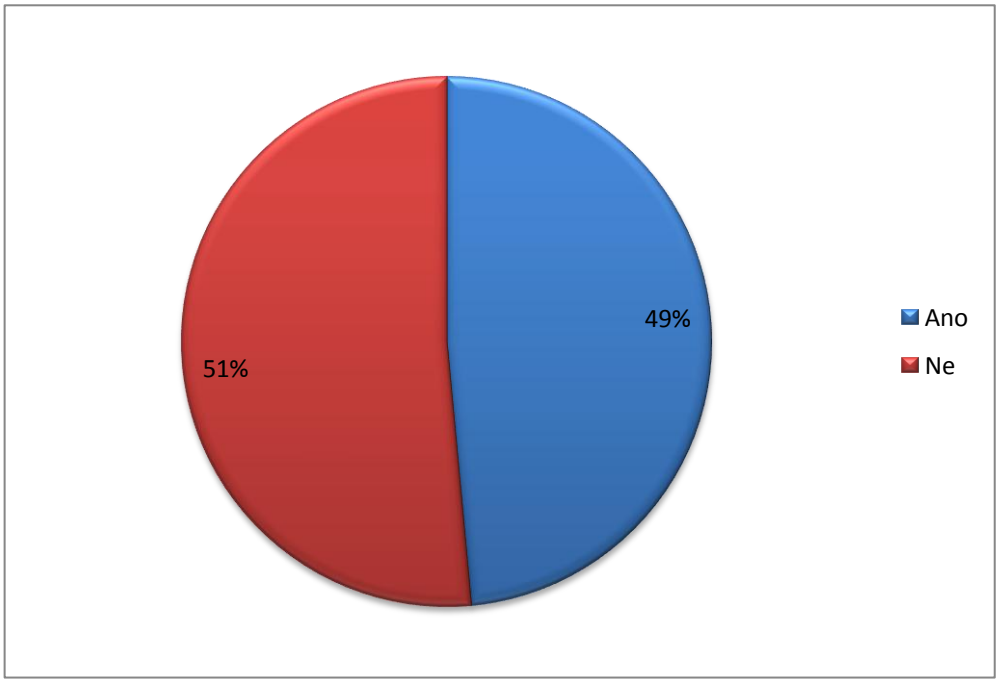
Možnosti výběru: Ano/Ne

Záměrem otázky bylo zjistit, zda studenti někdy zrušili registraci na sociální síti kvůli nevyhovujícím podmínkám.

Tab. 10 Zrušení registrace na sociální síti

Možnost výběru	Počet odpovědí	Odpovědi v %
Ano	33	48,53%
Ne	35	51,47%

[Zdroj: vlastní zpracování]



Obr. 11 Diagramové znázornění otázky č. 8 [Zdroj: vlastní zpracování]

Otázka č. 9: **Zveřejňujete o sobě na sociálních sítích soukromé informace?**

Výsledky odpovědí v procentech jsou uvedeny v tabulce číslo 11 a diagramově vyobrazeny na obrázku číslo 12.

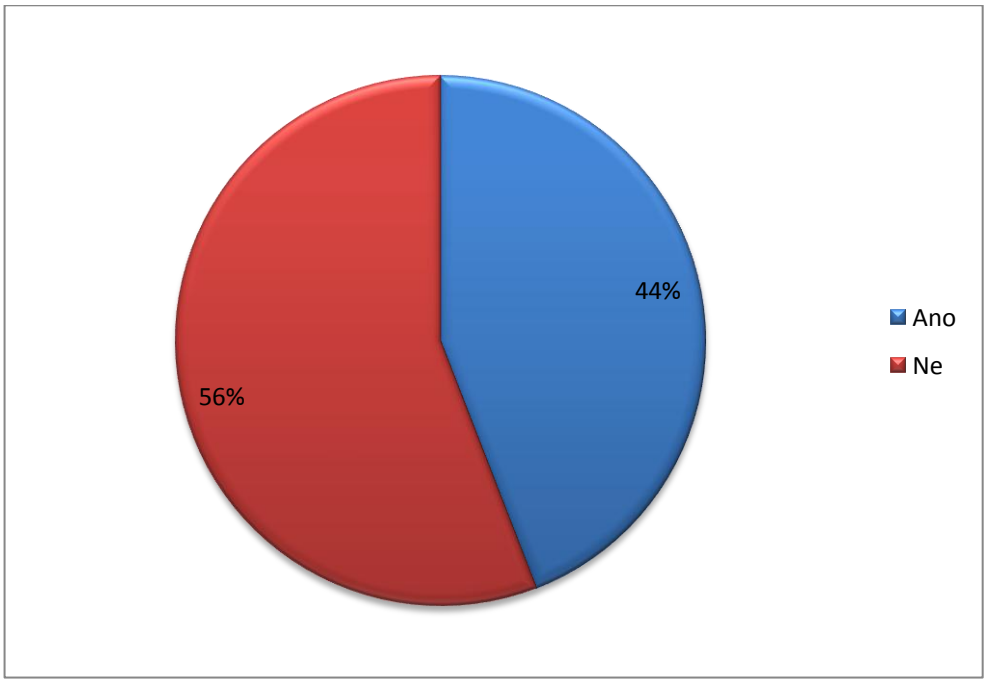
Možnosti výběru: Ano/Ne

Záměrem otázky bylo zjistit, zda studenti zveřejňují o sobě na sociálních sítích soukromé informace.

Tab. 11 Zveřejňování soukromých informací na sociálních sítích

Možnost výběru	Počet odpovědí	Odpovědi v %
Ano	30	44,12%
Ne	38	55,88%

[Zdroj: vlastní zpracování]



Obr. 12 Diagramové znázornění otázky č. 9 [Zdroj: vlastní zpracování]

Otázka č. 10: **Znáte možná rizika, která Vás na sociálních sítích mohou potkat?**

Výsledky odpovědí v procentech jsou uvedeny v tabulce číslo 12 a diagramově vyobrazeny na obrázku číslo 13.

Možnosti výběru: Ano, vyjmenujte/Ne

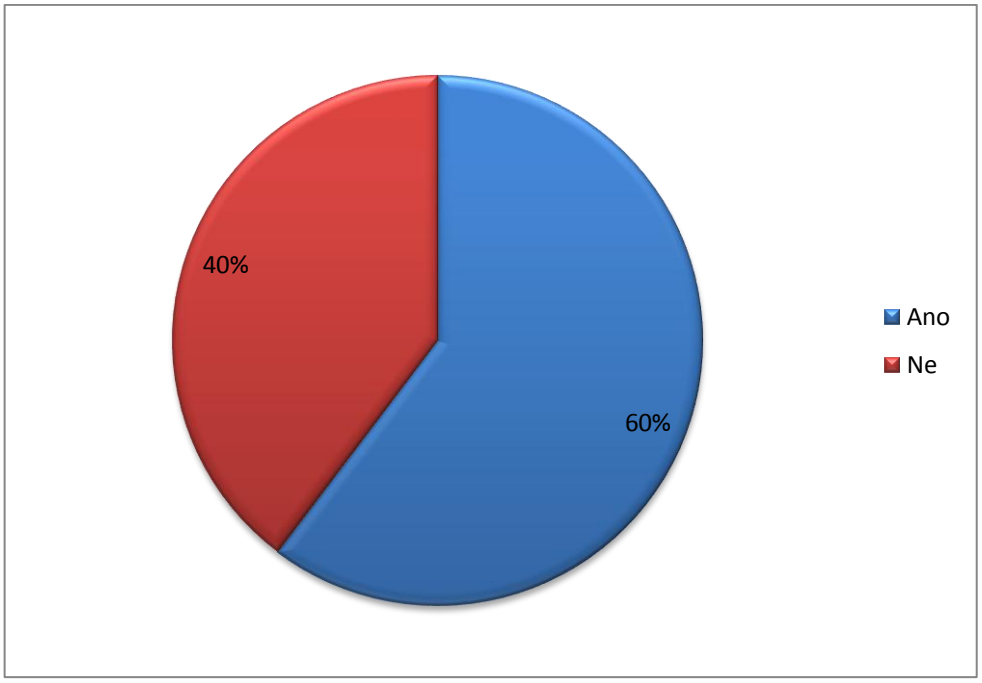
Záměrem otázky bylo zjistit, zda studenti znají možná rizika, která je mohou na sociálních sítích potkat. Respondenti, kteří odpověděli na otázku ano, vyjmenovali možná rizika, která je mohou potkat na sociálních sítích. U této otázky uvádím možné odpovědi některých respondentů:

- „Zneužití mých soukromých informací."
- „Zneužití mých fotografií."
- „Kyberšikana, pedofilie."
- „Obtěžování, sledování."
- „Někdo si Vás může vyhledat."

Tab. 12 Znalost možných rizik na sociálních sítích

Možnost výběru	Počet odpovědí	Odpovědi v %
Ano	41	60,30%
Ne	27	39,70%

[Zdroj: vlastní zpracování]



Obr. 13 Diagramové znázornění otázky č. 10 [Zdroj: vlastní zpracování]

Otázka č. 11: **Setkali jste se sami s internetovou šikanou nebo ve svém okolí?**

Výsledky odpovědí v procentech jsou uvedeny v tabulce číslo 13 a diagramově vyobrazeny na obrázku číslo 14.

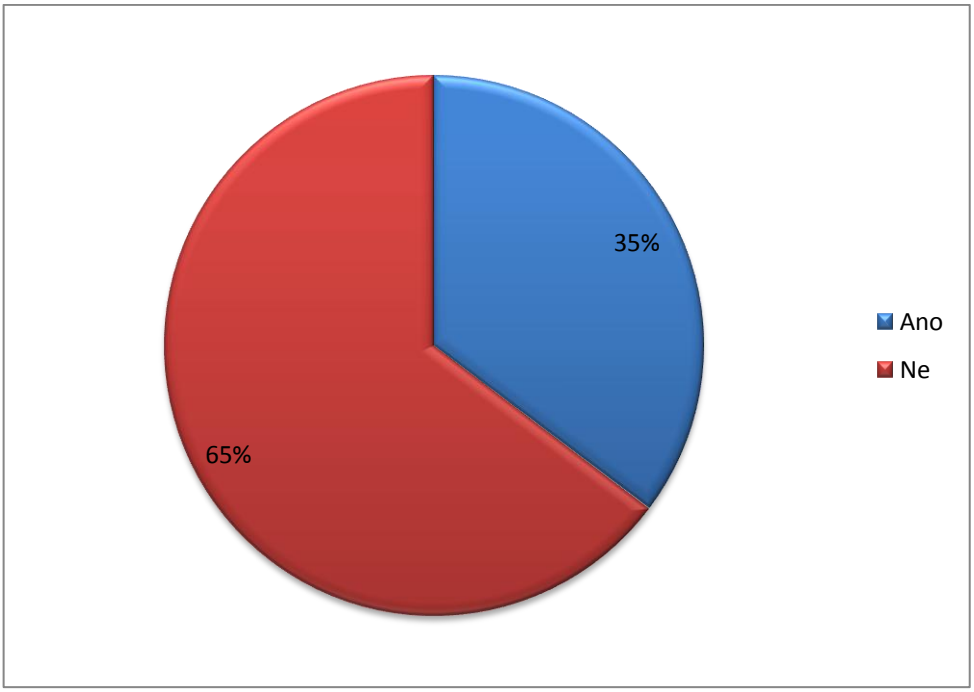
Možnosti výběru: Ano/Ne

Záměrem otázky bylo zjistit, zda se studenti sami setkali s internetovou šikanou nebo se s internetovou šikanou setkali ve svém okolí.

Tab. 13 Setkání s internetovou šikanou

Možnost výběru	Počet odpovědí	Odpovědi v %
Ano	24	35,30%
Ne	44	64,70%

[Zdroj: vlastní zpracování]



Obr. 14 Diagramové znázornění otázky č. 11 [Zdroj: vlastní zpracování]

Otázka č. 12: **Víte, jak se bránit útokům ze sociálních sítí?**

Výsledky odpovědí v procentech jsou uvedeny v tabulce číslo 14 a diagramově vyobrazeny na obrázku číslo 15.

Možnosti výběru: Ano, vyjmenujte/Ne

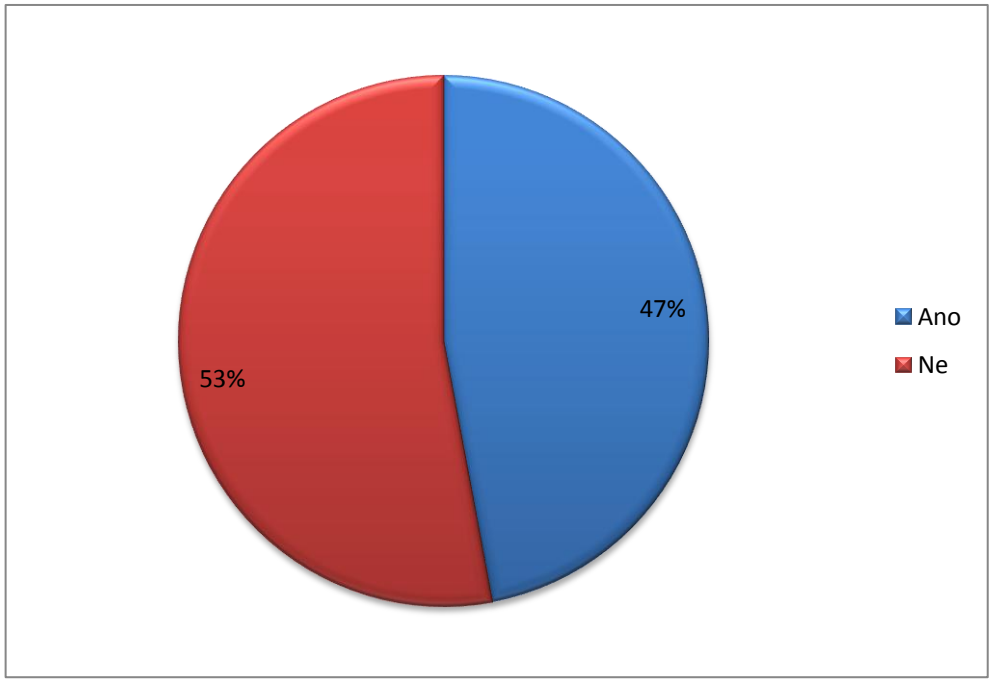
Záměrem otázky bylo zjistit, zda studenti vědí, jak se bránit útokům ze sociálních sítí. Respondenti, kteří odpověděli na otázku ano, vyjmenovali možné útoky, které je mohou potkat na sociálních sítích. U této otázky uvádím možné odpovědi některých respondentů:

- „Zablokovat, zrušit účet na sociální síti.“
- „Nepodávat soukromé informace.“
- „Nahlásit útoky na policii.“
- „Stačí nebýt neopatrný.“
- „Každý má nějaké řešení.“

Tab. 14 Znalost obrany proti útokům ze sociálních sítí

Možnost výběru	Počet odpovědí	Odpovědi v %
Ano	32	47,06%
Ne	36	52,94%

[Zdroj: vlastní zpracování]



Obr. 15 Diagramové znázornění otázky č. 12 [Zdroj: vlastní zpracování]

Otázka č. 13: **Která věková skupina je podle Vás při užívání sociálních sítí nejvíce ohrožena?**

Výsledky odpovědí v procentech jsou uvedeny v tabulce číslo 15 a diagramově vyobrazeny na obrázku číslo 16.

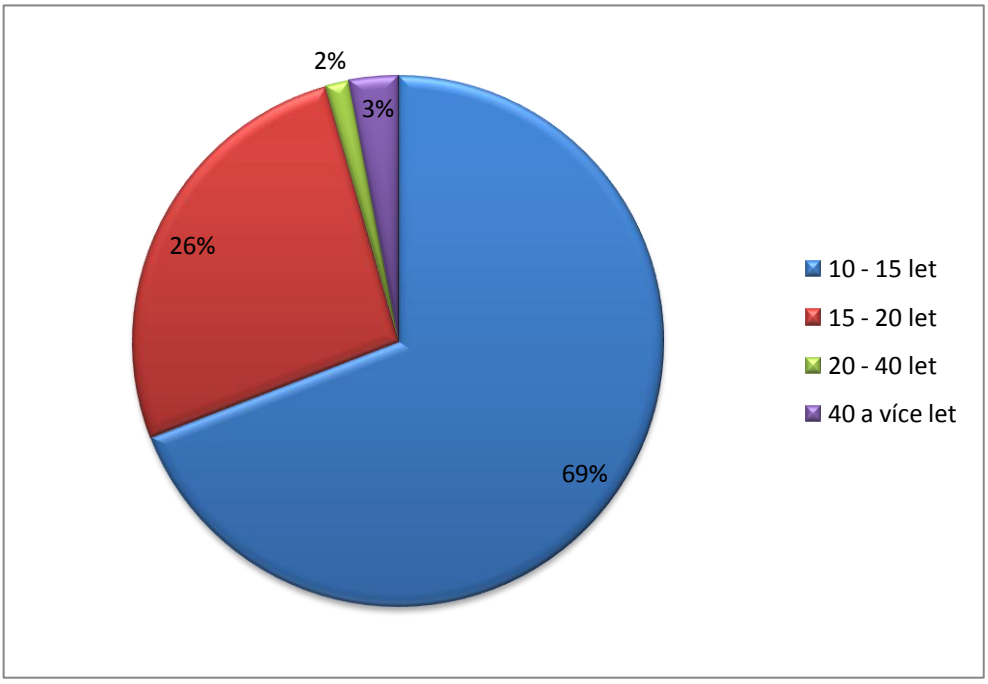
Možnosti výběru: 1 ze 4

Záměrem otázky bylo zjistit, která věková skupina je podle studentů při užívání sociálních sítí nejvíce ohrožena.

Tab. 15 Ohrožená věková skupina na sociálních sítích

Možnost výběru	Počet odpovědí	Odpovědi v %
10 – 15 let	47	69,12%
15 – 20 let	18	26,47%
20 – 40 let	1	1,47%
40 a více let	2	2,94%

[Zdroj: vlastní zpracování]



Obr. 16 Diagramové znázornění otázky č. 13 [Zdroj: vlastní zpracování]

Otázka č. 14: **Myslíte si, že Vám bylo doma, ve škole či zaměstnání dostatečně vysvětleno nebezpečí sociálních sítí?**

Výsledky odpovědí v procentech jsou uvedeny v tabulce číslo 16 a diagramově vyobrazeny na obrázku číslo 17.

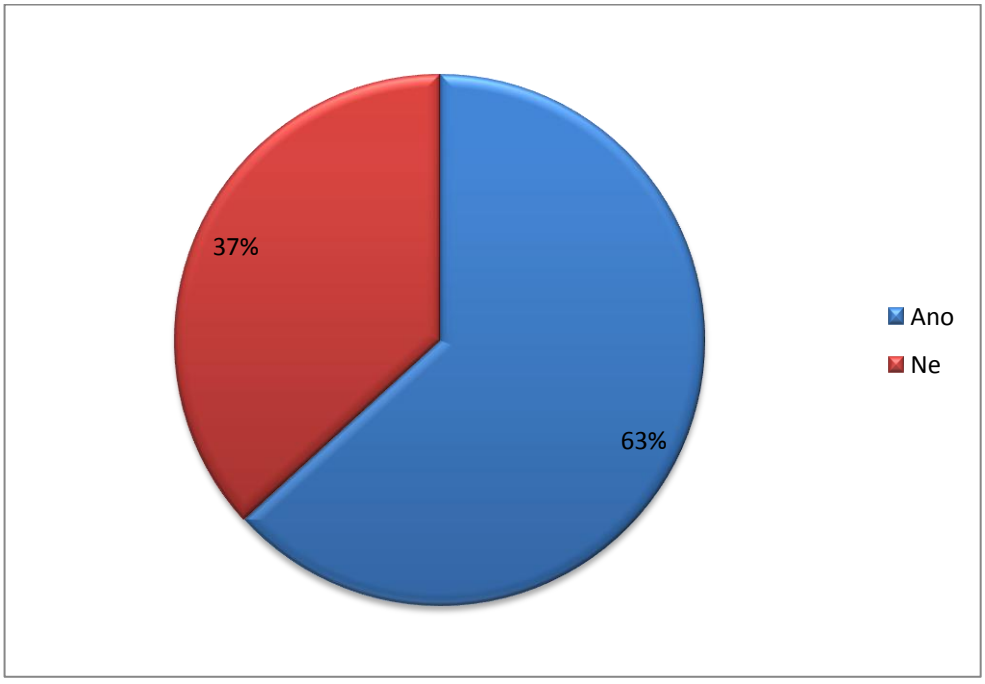
Možnosti výběru: Ano/Ne

Záměrem otázky bylo zjistit, jestli bylo studentům doma nebo ve škole dostatečně vysvětleno nebezpečí, se kterým se mohou potkat na sociálních sítích.

Tab. 16 Vysvětlení nebezpečí s užíváním sociálních sítí

Možnost výběru	Počet odpovědí	Odpovědi v %
Ano	43	63,24%
Ne	25	36,76%

[Zdroj: vlastní zpracování]



Obr. 17 Diagramové znázornění otázky č. 14 [Zdroj: vlastní zpracování]

Otázka č. 15: **Provedli jste nějaká opatření k zabezpečení Vašeho počítače nebo Vaší osoby proti útokům ze sociálních sítí?**

Výsledky odpovědí v procentech jsou uvedeny v tabulce číslo 17 a diagramově vyobrazeny na obrázku číslo 18.

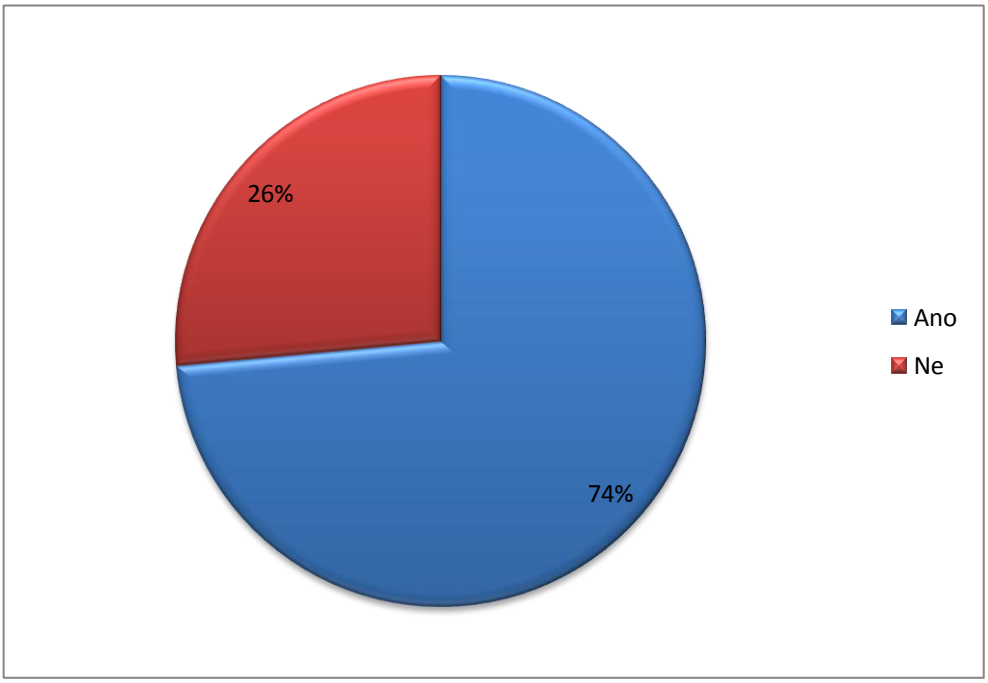
Možnosti výběru: Ano/Ne

Záměrem otázky bylo zjistit, jestli studenti provedli nějaká opatření týkající se zabezpečení jejich počítače nebo jejich osoby proti útokům ze sociálních sítí.

Tab. 17 Provedení zabezpečení počítače

Možnost výběru	Počet odpovědí	Odpovědi v %
Ano	50	73,53%
Ne	18	26,47%

[Zdroj: vlastní zpracování]



Obr. 18 Diagramové znázornění otázky č. 15 [Zdroj: vlastní zpracování]

5.2 Shrnutí dotazníkového šetření

Uskutečněným kvantitativním výzkumem jsme zamýšleli zjistit, jaké jsou tendence v užívání Internetu. Počítač s připojením k Internetu má 100% studentů. Můžeme tedy říct, že se dnes stal jejich součástí. Studenti využívají počítač k zábavě a to ve 39,70% případů. Tento výsledek nám dává odpověď, že dospívající studenti tráví na sítí většinu času. Další tendencí, které si lze všimnout z odpovědí respondentů je, že znají, navštěvují sociální sítě každý den a to ve 94,12%, registrováno na některé z nich je 100% respondentů. Dále nás zajímalo, zda respondenti si prostudovali podmínky registrace ať už při zakládání sociální sítě nebo při změně podmínek po aktualizaci a zda někdy kvůli nevyhovujícím podmínkám registraci zrušili. Podmínky si prostudovalo jen 26,47% studentů, registraci kvůli nevyhovujícím podmínkám zrušilo 48,53% studentů.

Pozoruhodným zjištěním nepochybně je zveřejňování, sdílení soukromých informací na sítích. Respondenti na své osobní informace nejsou obezřetní, poněvadž celých 55,88% má nějakou z těchto informací na Internetu dostupně uveřejněnou.

Dále nás zajímalo, zda respondenti znají možná rizika, která mohou na sociálních sítích potkat a jestli se někdy setkali s internetovou šikanou, zda vědí, jak by se bránili v těchto rizikových situacích. Více jak polovina respondentů (60,30%) zná možná rizika, která je mohou potkat na sociálních sítích a 35,30% respondentů se již setkala se situací, kdy se je někdo snažil šikanovat. Za hodně rizikové lze uvést fakt, že jen 47,06% ví, jak se bránit útokům ze sociálních sítí. Nejvíce ohroženou věkovou skupinou při užívání sociálních sítí je podle respondentů věková skupina 10 – 15 let a to v 69,12% případů.

Dále nás zajímalo, jestli jsou respondenti poučeni o nebezpečí, které hrozí na sociální síti a jestli provedli nějaká opatření k zabezpečení počítače proti útokům ze sociálních sítí. Zjistili jsme, že poučeni o nebezpečí na sociální síti jsou respondenti v 63,24% a opatření provedlo 73,53% respondentů.

ZÁVĚR

V dnešním moderním světě je Internet podstatnou součástí naše života. Nabízí služby, mezi které patří vyhledávání informací, nakupování, zábavu a další. Komunikace je rychlá, efektivní, levná. Kontakt s přáteli, obchodními partnery, rodinou může být v kteroukoli hodinu.

Komunikace na Internetu obnáší nemalá rizika. Uživatelé sociálních sítí ještě nepochytili, jak nakládat s těmito komunikačními nástroji. Mnoho uživatelů má na svém profilu zveřejněny osobní informace, které jsou přístupné i cizím návštěvníkům. Sociální sítě jsou zásobárnou soukromých informací, které mohou být zneužity k různým podvodům.

SWOT analýzou jsme došli k závěru, že největší hrozbou je zneužití účtu, krádež identity, která může nastat při nedostatečném zabezpečení sociální sítě. Uživatelé by se měli soustředit na zabezpečení účtu své sociální sítě.

Dotazníkové šetření poukázalo také na problém spojený s neznalostí způsobů ochrany před hrozbami zneužití sociálních sítí. Většina uživatelů sociálních sítí zná možná rizika, ale neví jak se bránit proti útokům ze sociálních sítí. Další zjištění poukazuje na velké množství osobních údajů zveřejňovaných vlastníky účtu bez dostatečného omezení jejich dostupnosti pro cizí uživatele. Přičemž možnou ochranou je omezení dostupnosti těchto dat pro cizí uživatele sociálních sítí.

Někteří uživatelé mají nepochopitelné a nezodpovědné chování, proto se mohou stát cílem pro počítačové zločince, kteří mohou ukradnout jejich identitu a osobní údaje. Zločinci užívají jednoduché nástroje a psychologické triky. Zcizenou identitu využívají k obohacení.

Proto je nutné se zajímat o informace, které nám pomohou minimalizovat riziko, aby citlivé informace nebyly zneužity. Kromě vlastního nastavení soukromí, přemýšlet o tom, jaké informace o sobě sdělujeme neznámým osobám. V neposlední řadě aktualizací počítače podstatně snížit možnost vniknutí hackerů do počítače.

SEZNAM POUŽITÉ LITERATURY

[1] BURIAN, Pavel. *Internet inteligentních aktivit*. Vyd. 1. Praha: Grada, 2014, 332 s. Průvodce (Grada). ISBN 978-80-247-5137-5.

[2] DOUCEK, Petr, Luděk NOVÁK a Vlasta SVATÁ. *Řízení bezpečnosti informací*. 1. vyd. Praha: Professional Publishing, 2008, 239 s. ISBN 978-80-86946-88-7.

[3] ECKERTOVÁ, Lenka a Daniel DOČEKAL. *Bezpečnost dětí na internetu: rádce zodpovědného rodiče*. 1. vyd. Brno: Computer Press, 2013, 224 s. ISBN 978-80-251-3804-5.

[4] HLAVENKA, Jiří. *Internet*. Vyd. 1. Brno: Computer Press, 2003, iv, 196 s. Vizuální příručka nové generace. ISBN 80-7226-988-7.

[5] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

[6] PAVLÍČEK, Antonín. *Nová média a sociální sítě*. Vyd. 1. Praha: Oeconomica, 2010, 181 s. ISBN 978-80-245-1742-1.

[7] PEACOCK, Michael. *Programujeme vlastní sociální síť v PHP 5*. 1. vyd. Brno: Computer Press, 2012, 424 s. ISBN 978-80-251-3626-3.

[8] ŠTĚDROŇ, Bohumír a Miroslav LUDVÍK. *Právo v informačních technologiích*. Vyd. 1. Kralice na Hané: Computer Media, 2008, 132 s. ISBN 978-80-86686-36-3.

[9] WALTER, Ekaterina. *Mysli jako Zuckerberg: pět podnikatelských tajemství šéfa firmy Facebook*. Vyd. 1. Praha: Management Press, 2013, 239 s. Knihovna světového managementu. ISBN 978-80-7261-264-2.

[10] ZELENÝ, Jaroslav a Božena MANNOVÁ. *Historie výpočetní techniky*. 1. vyd. Praha: Scientia, 2006, 183 s. Stručné dějiny oborů. ISBN 80-86960-04-8.

[11] Zákon o ochraně osobních údajů. [online]. [cit. 2015-02-10]. Dostupné z: http://business.center.cz/business/pravo/zakony/oou/

[12] Obchodní podmínky pro poskytování služby elektronického bankovnictví. [online]. [cit. 2015-02-11]. Dostupné z: http://www.csob.cz/WebCsob/Csob/Obchodni-podminky/Podminky_CSOB_BB24_cz_150101.pdf

[13] Nové podmínky užívání Facebooku. [online]. [cit. 2015-02-11]. Dostupné z: http://zpravy.aktualne.cz/ekonomika/technika/facebook-vas-sleduje-ale-co-skutecne-meni-od-noveho-roku/r~6e42357e877e11e49fc3002590604f2e/

[14] Internetový prodej trhá rekordy. [online]. [cit. 2015-02-13]. Dostupné z: http://www.novinky.cz/finance/334400-internetovy-prodej-trha-rekordy-lide-si -pro -zbozi-chodi-osobne-a-plati-hotove.html

[15] Mezinárodní organizace pro normalizaci. [online]. [cit. 2015-02-13]. Dostupné z: http://cs.wikipedia.org/wiki/Mezin%C3%A1rodn%C3%AD_organizace_pro_normalizaci

[16] Systémy ISO. [online]. [cit. 2015-02-15]. Dostupné z: http://www.mbk.cz/iso-27001

[17] ISO normy. [online]. [cit. 2015-04-15]. Dostupné z: http://www.noveiso.cz/iso _27001.html

[18] Projekt E-Bezpečí. [online]. [cit. 2015-04-16]. Dostupné z: http://www.e-bezpeci. cz/index.php/o-projektu/oprojektu

[19] Kyberšikana. [online]. [cit. 2015-04-20]. Dostupné z: http://www.e-bezpeci.cz/ index.php/temata/kyberikana

[20] Kyberstalking. [online]. [cit. 2015-04-21]. Dostupné z: http://www.e-bezpeci.cz/ index.php/temata/stalking-a-kyberstalking

[21] Sexting. [online]. [cit. 2015-04-23]. Dostupné z: http://www.e-bezpeci.cz/index. php/temata/sexting

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ARPA	Advance Research Projects Agency
CERN	Evropská organizace pro nukleární výzkum
.com	Generická doména nejvyššího řádu
EARN	European Academic and Research Network
HTTP	HyperText Transfer Protocol
HTML	HyperTex Markup Language
IBM	International Business Machines Corporation
ISO	International Organization for Standardization
NSF	National Science Foundation
.org	Generická doména nejvyššího řádu
PDCA	Plan-do-check-act
SMS	Short message service
TCP/IP	Transmission Control Protocol/Internet Protocol
USA	United States of America
WWW	World Wide Web

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK

Milá studentko, milý studente,

Jmenuji se Šárka Buberová a studuji poslední ročník bakalářského studia fakulty logistiky a krizového řízení UTB Zlín. Tento dotazník je vytvořen pro mou závěrečnou práci, která se zabývá riziky na internetových sociálních sítích. Hlavním cílem je zjistit, jaké jsou Vaše zkušenosti s používáním Internetu a povědomí o možných rizicích, která jsou spojena s jeho užíváním. Dotazník je anonymní. Prosím vás o otevřenost při jeho vyplňování. Vyplněný dotazník, prosím, vraťte co nejdříve předavateli. Děkuji.

Jsem: žena ☐ muž ☐ (označte prosím křížkem)

Můj věk: ……

Vzdělání:……

Postup při vyplňování dotazníku: zakroužkujte vždy jednu odpověď, pokud není uvedeno jinak.

1. **Máte doma počítač s připojením k internetu?**
   a) Ano
   b) Ne
2. **K jakému účelu počítač doma převážně využíváte?**
   a) Škola
   b) Práce
   c) Zábava
3. **Které nejznámější sociální sítě znáte? (můžete označit více odpovědí, případně doplnit)**
   a) Facebook
   b) Twitter
   c) MySpace
   d) LinkedIn
   e) Google+
   f) Jiné (vypište)……
4. **Které české sociální sítě znáte? (můžete označit více odpovědí, případně doplnit)**
   a) Lidé.cz
   b) Spolužáci.cz
   c) Líbímseti.cz
   d) SitIT.cz
   e) SportCentral.cz
   f) ČSFD.cz
   g) Jiné (vypište)……

5. **Kolik sociálních sítí využíváte?**
   a) 0
   b) 1
   c) 2
   d) 3 a více
6. **Jak často navštěvujete Vaši sociální síť?**
   a) Každý den
   b) 2x - 3x za týden
   c) 1x za měsíc
7. **Prostudovali jste si důkladně podmínky registrace na sociální síti nebo změny podmínek po aktualizaci?**
   a) Ano
   b) Ne
   c) Nepamatuji se
8. **Zrušili jste někdy registraci kvůli nevyhovujícím podmínkám?**
   a) Ano
   b) Ne
9. **Zveřejňujete o sobě na sociálních sítích soukromé informace?**
   a) Ano
   b) Ne
10. **Znáte možná rizika, která Vás na sociálních sítích mohou potkat? Pokud ano, vyjmenujte.**
    a) Ano

    .....

    b) Ne
11. **Setkali jste se sami s internetovou šikanou nebo ve svém blízkém okolí?**
    a) Ano
    b) Ne
12. **Víte, jak se bránit útokům ze sociálních sítí? Pokud ano, vyjmenujte.**
    a) Ano

    ……

    b) Ne
13. **Která věková skupina je podle Vás při užívání sociálních sítí nejvíce ohrožena?**
    a) 10 - 15 let
    b) 15 - 20 let
    c) 20- 40 let
    d) 40 a více let

14. **<u>Myslíte si, že Vám bylo doma, ve škole či zaměstnání dostatečně vysvětleno nebezpečí sociálních sítí?</u>**
    a) Ano
    b) Ne
15. **<u>Provedli jste nějaká opatření k zabezpečení Vašeho počítače nebo Vaší osoby proti útokům ze sociálních sítí?</u>**
    a) Ano
    b) Ne

Děkuji vám za vyplnění a Váš čas!!!