VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

BEZPEČNOSTNÍ RIZIKA SOCIÁLNÍCH SÍTÍ A JEJICH PREVENCE

SECURITY RISKS OF SOCIAL NETWORKS AND THEIR PREVENTION

DIPLOMOVÁ PRÁCE

DIPLOMA'S THESIS

AUTOR PRÁCE — **Bc. Sao Linh Nguyen**

AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**

SUPERVISOR

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Sao Linh Nguyen**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2017/18

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Bezpečnostní rizika sociálních sítí a jejich prevence

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska
Analýza současného stavu
Vlastní návrh řešení
Zhodnocení a přínosy práce
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem práce je analyzovat bezpečnostní hrozby a rizika online sociálních sítí a navrhnout preventivní opatření k jejich prevenci.

Základní literární prameny:

KAVALÍR, A. Kyberšikana a její prevence. Plzeň: Dragon Press, 2009. ISBN 978-80-86961-78-1.

KOPECKÝ, K. a V. KREJČÍ. Rizika virtuální komunikace. Olomouc: Net University, 2010. ISBN 978-80-254-7866-0.

ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

PAVLÍČEK, A. Nová média a sociální sítě. Praha: Nakladatelství Oeconomica, 2010. ISBN 978-8--245-1742-1.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2017/18

V Brně dne 28.2.2018

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Diplomová práce pojednává o fenoménu internetových sociálních sítí. Cílem práce je podat základní informace o sociálních sítích – přehled a charakteristika nejrozšířenějších sociálních sítí, poukázat na riziko spjaté s jejich používáním a doporučit uživatelům jejich bezpečné používání.

Klíčová slova

Sociální sítě, Facebook, Instagram, YouTube, LinkedIn, seznam rizik, analýza rizik, zhodnocení, doporučení pro uživatele.

Abstract

The diploma thesis deals with the phenomenon of internet social networks. The aim of the work is to provide basic information about social networks – overview and characteristics of the most widespread social networks, to point out the risk associated with their use and to recommend users to use them safely.

Keywords

Social networking, Facebook, Instagram, YouTube, LinkedIn, risk list, risk analysis, evaluation, user recommendations.

Bibliografická citace

Nguyen, SL. *Bezpečnostní rizika sociálních sítí a jejich prevence.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2018. 78 s. Vedoucí diplomové práce Ing Petr Sedlák

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 20. května 2018

……

podpis

Poděkování

Tímto bych rád poděkoval vedoucím diplomové práce panu Petrovi Sedlákovi za cenné poznatky a odborné rady, které mi pomohly při tvorbě této diplomové práce. Také bych chtěl poděkovat své rodině za trpělivost a podporu po celou dobu studia.

ÚVOD

Sociální sítě se staly v desátých letech 21 století globálním fenoménem. V současné době jsou sociální sítě nejpoužívanější internetovou službou. Na konci roku 2017 používaly sociální sítě více než 2,4 miliardy lidí po celém světě a jejich počet neustále roste. Uživatelé po celém světě jsou ke svým oblíbeným sociálním sítím připojeni téměř nepřetržitě. Sociální sítě představují velice užitečný a univerzální nástroj, díky kterému má uživatel možnost rychlé komunikace a sdílení různých aktivit s určitou, jím zvolenou skupinou lidí. Základem sociálních sítí byla interakce mezi uživateli, kteří navzájem komunikovali prostřednictvím virtuálních uživatelských profilů. Mezi hlavní přínosy sociálních sítí patří především zábava, komunikace, vzdělání, ale také marketing a propagace firmy či fyzické osoby.

Existuje obrovské množství sociálních sítí, proto budou rozebrány ty sociální sítě, které jsou momentálně nejpoužívanější. K těmto sítím můžeme zařadit Facebook, Twitter, Instagram a LinkedIN. Sociální sítě jsou mocným a užitečným nástrojem, nicméně na nich existuje obrovské množství hrozeb. Účelem této diplomové práce je vytvořit seznam hrozeb, které reálně hrozí sociálním sítím, jejím provozovatelům a uživatelům. Následně stanovit velikost rizik na základě dopadů, frekvence výskytu a úspěšnosti hrozeb. Vůči hodnoceným rizikům pak stanovit opatření, prostřednictvím kterých lze hodnocená rizika zmírnit, eliminovat nebo se rizikům vyhnout.

1 CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Subjekt, kterého se týkají zpracovávaná data v této diplomové práci, si nepřeje zveřejnit svůj název. V práci tedy bude tato společnost uváděn jako „popisovaná firma“ nebo „popisovaný subjekt“.

1.1 Cíle práce

Cílem práce je zjistit nedostatky a bezpečnostní hrozby uživatelských účtů na nejpoužívanějších sociálních sítích a dopady těchto nedostatků na samotné uživatele. V praktické části diplomové práce jsou navržena řešení, které má za úkol zvýšit povědomí uživatelů popisované firmy o zabezpečení a doporučení pro eliminaci analyzovaných hrozeb.

1.2 Metody a postup zpracování

Metodika zpracování této diplomové práce se skládá z těchto kroků:

- Vysvětlení základních pojmů a seznámení s nejznámějšími sociálními sítím;
- Sestavení seznamu hrozeb sociálních sítí;
- Provedení analýza rizik sociálních sítí;
- Zhodnocení analýzy rizik;
- Sestavení bezpečnostních doporučení a opatření pro uživatele sociálních sítí.

V kapitole Rizika a hrozby sociálních sítí je probrán výčet možných hrozeb, které ohrožují uživatele sociálních sítí. Seznam hrozeb je čerpán z veřejně dostupných zdrojů, které o incidentech spojených se sociálními sítěmi informují, dále z praktických zkušeností uživatelů popisovaného podniku.

V kapitole Analýza rizik jsou na základě seznamu hrozeb, jejich možného negativního dopadu, pravděpodobnosti výskytu a úspěšnosti hrozeb vypočtena rizika, která z uvedených hrozeb vyplývají.

V kapitole Zhodnocení jsou vyhodnocena rizika a dopady, které mohou rizika způsobit, pokud dojde k jejich reálnému naplnění.

Kapitola Doporučení pro uživatele je věnována návrhům obecných i konkrétních opatření. Díky opatřením by měl být uživatel schopen výše zmíněná rizika buď zcela potlačit, nebo alespoň částečně zmírnit, případně se rizikům vyhnout.

2 TEORETICKÁ VÝCHODISKA

Tato část práce je věnována popisům základní pojmů, kterých bude následně využito pro zpracování analytické a praktické části práce.

2.1 Internet

Internet je propojení jednotlivých počítačů pomocí síťových prvků a kabelů, kdy tyto počítače mezi sebou komunikují pomocí protokolů. Internet je pro lidstvo obrovských přínosem. Dá se říci, že lidem hodně usnadňuje práci. Dříve člověk musel složitě hledat v knihách, chodit za zkušenějšími lidmi apod. V současné době si pouze otevře internetový prohlížeč, zadá do něj klíčové slovo a už mu „vybíhá“ nepřeberné množství odkazů k zadanému slovu či tématu. Zároveň je však nutné, abychom s ním uměli zacházet, znali jeho klady, ale hlavně i jeho zápory a nebezpečí, která na něm číhají a jak těmto hrozbám předcházet, případně když už k nějakému reálnému ohrožení dojde, jak v takové situaci postupovat. (1)

2.2 Kyberprostor

Kyberprostor je virtuální počítačový svět, přesněji elektronické médium tvořící světovou, globální počítačovou síť, která je základem online komunikace. Je to rozsáhlá počítačová síť tvořena menšími, po světě rozesetými počítačovými sítěmi, které užívají TCP/IP protokol. Ten jim umožňuje komunikaci a výměnu dat.

Jedna z hlavních vlastností struktury kyberprostoru je otevřenost širokému okruhu uživatelů v interaktivní a virtuálním prostředí. Další vlastností je anonymita, ta umožňuje v podstatě jakékoliv jednání bez zodpovědnosti.

Kyberprostor umožňuje uživatelům komunikovat, sdílet a vyměňovat si informace a nápady, hrát hry, účastnit se diskuzí na sociálních fórech, provádět obchodní transakce. (2)

2.2.1 Definice hrozby

HROZBA je hrozivá blízkost něčeho zlého, tedy jevu, události, procesu, který svými projevy, faktory, intenzitou a následky omezuje, ohrožuje, ničí, devastuje a likviduje životy, zdraví, majetek, životní prostředí, kulturní hodnoty. Hrozba vždy působí v konkrétním čase, místě a na konkrétní objekty a subjekty.

Hrozby mají tři fáze:

a) existence hrozby – víme o existenci jevu, události, procesu, nebo činnosti, ale době hmoty, síly a energie jsou v rovnováze, pouze může dojít k určitým deformacím, výkyvům, anomáliím, kolísání hmot, sil a energií;
b) působení hrozby – vznikla mimořádná událost, nebo krizová situace, je narušena rovnováha hmot, sil a energií jejich akumulací, či úbytkem, nebo došlo k expanzi nárůstu a k neřízenému uvolnění (uvolňování), nebo neřízené, náhlé (postupné) regresi, či úbytku hmot, sil a energií;
c) zánik hrozby – faktory (fyzikální, chemické, biologické, společenské) hrozby přestávají působit. Dochází k odstraňování deformací a adaptaci hmot, sil a energií po jejich uvolnění, či úbytku, je obnovována rovnováha hmot, sil a energií a vzniká nová rovnováha hmot, sil a energií.

Hrozba existuje pouze když existuje riziko. Tedy pravděpodobnost vzniku negativního jevu, události, procesu, nebo činnosti (mimořádné události, krizové situace) musí být větší než nula a zároveň ale i následky musí být větší než nula.

Pochopení nebezpečí, rizik a hrozeb je v krizovém managementu velmi důležité, protože jejich analýza je základem pro havarijní, krizové a obranné plánování. (3)

2.2.2 Definice rizika

Původ výrazu riziko pochází údajně ze sedmnáctého století, kde byl používán v souvislosti s lodní plavbou a nebezpečím, kterému se museli mořeplavci vyhnout. S odstupem času se objevuje i ve vztahu k možné ztrátě. Pro účely normy ČSN ISO 31000 bylo riziko definováno následujícím způsobem:

- Riziko je pravděpodobnost nežádoucí události s nežádoucími následky.

V poznámce k chápání této definice se dále uvádí: *„Účinek je odchylka od očekávaného, kladná a/nebo záporná. Cíle mohou mít různá hlediska (jako jsou finanční, zdravotní, bezpečnostní a environmentální) a mohou být uplatňovány na různých úrovních“*

Z definice normy vyplývá:

- s rizikem je spojená vždy nejistota neboli pravděpodobnost;
- nezbytný účinek nejistoty, který je spojen s rizikem;
- vztah k dosažení cílů, tedy i kroků k dosažení cílů.

Jinými slovy můžeme taky jednoduše tvrdit, že riziko je vlastnost hrozby. (3)

2.3 Sociální sítě

Sociální síť je internetová služba, která slouží uživatelům k vytvoření osobního, či firemního profilu. Takovýto profil je podle nastavení uživatele a použité sociální sítě veřejný, nebo z části veřejný a umožňuje svému vlastníkovi, nebo správci, navazovat virtuální vztahy s ostatními uživateli. Sociální síť pak umožňuje propojeným uživatelům vzájemnou komunikaci, sdílení informací, fotografií, videí, odkazů, událostí a mnoho dalších aktivit. Existuje velké množství sociálních sítí, které se liší především v zaměření na určité funkční požadavky uživatelů.

Pro firmy jsou sociální sítě velmi účinným a používaným marketingovým nástrojem pro propagaci firmy a nabízených produktů. Sociální sítě jsou součástí každodenního života a v několika případech byly také použity jako důkaz při soudním sporu, kde byla použita jako důkaz fotografie, nebo komunikace mezi uživateli.

Sociální sítě jsou často označovány jako nová generace internetových služeb, tzv. web 2.0. Principem této nové generace World Wide Webu (www) je vytváření obsahu uživateli. Mezi hlavní představitele webu 2.0 patří právě sociální sítě jako Facebook, YouTube a Twitter spolu s Google. (4)

2.3.1 Facebook

Facebook je celosvětovým fenoménem. Jedná se o nejpoužívanější sociální síť, která měla v květnu roku 2018 2,05 miliardy aktivních uživatelů. Úkolem Facebooku je dát lidem možnost sdílet informace a dělat tak svět více propojeným. Lidé používají Facebook, aby mohli zůstat v kontaktu s přáteli a rodinou, a aby zjistili, co je nového ve světě a sdíleli to, na čem jim záleží. Informace pro zpracování této podkapitoly byly získány z oficiálních stránek a centra nápovědy Facebooku. (5)

2.3.1.1 Vznik Facebooku

Facebook byl založen studentem Harvadu Markem Zuckerbergem a jeho spolužáky Eduardem Saverinem, Dustinem Moskovitzem a Chrisem Hughesem. Jejich původním projektem byl Facemash, který se v mnohém podobal dnešnímu Tinderu. Jednalo se o výběr přitažlivější studentky/studenta ze dvou možností. Aby tento projekt mohl vůbec začít, byla potřeba databáze studentů Harvardu. Tu Zuckerberg získal tak, že se naboural do sítě Harvardu. Projekt byl spuštěn 28. 10. 2003 a odstaven o několik dní později úředníky Harvardu z důvodu zneužití osobních údajů. Mark Zuckerberg byl obviněn z porušení bezpečnosti, autorských práv a práv jednotlivce za krádeže snímků studentů,

použitých na stránkách Facemash. V důsledku těchto obvinění čelil Zuckerberg vyloučení z Harvardské university, nicméně všechna obvinění byla stažena a Zuckerberg dostal pouze podmíněné vyloučení po dobu půl roku. (5)

Nové stránky pod názvem Thefacebook Zuckerberg spustil 4. 2. 2004. Název Thefacebook vznikl podle názvu seznamovacích letáků amerických studentů. 10. 2. 2004 čelil obvinění od tří studentů Harvardu, Camerona Winklevosse, Tylera Winklevosse a Divya Narendra, že jejich nápad ukradl. Jednalo se jim o velkou podobnost projektů HarvardConnection, na kterém s dvojčaty Winklevossovými a Narendrou pracoval, a Thefacebook. Všechny spory však byly vyřešeny mimosoudní cestou a Zuckerberg zaplatil minimálně 65 miliónů dolarů odškodné. TheFacebook byl původně pouze pro studenty Harvardu ale postupem času se Zuckerberg rozhodl zaměstnat několik svých spolužáků a expandovat na další univerzity a vysoké školy. V roce 2004 vstoupil do společnosti investor Sean Parker, který navrhl odkoupení domény facebook.com za 200 000 dolarů. Společnost tak dostala nové jméno Facebook. (6)

Celý příběh Marka Zuckerberga a vzniku Facebooku byl zachycen ve snímku "The Social Network" režiséra Davida Finchera. Od tohoto filmu se však firma Facebook i samotný Mark Zuckerberg distancovali. (7)

2.3.1.2 Software Facebooku

Jelikož Facebook operuje s velkým množstvím dat, některé tradiční přístupy a technologie nejsou praktické. Úkolem vývojářů Facebooku je zajistit hladký běh služby pro více než miliardu aktivních uživatelů. (9)

LAMP

Základním stavebním kamenem je LAMP software, což je open-source software skládající se v případě Facebooku z operačního systému Linux, webového serveru Apache, databázového systému MySQL a skriptovacího programovacího jazyku PHP. Nicméně vývojáři Facebooku tyto jednotlivé části neustále vylepšují a rozšiřují o nové služby, díky kterým je aplikace mnohem výkonnější. Pro zrychlení běhu aplikace používá Facebook také Memcached a další služby a systémy. (9)

Memcached

Memcached je hojně používaným softwarovým řešením pro větší weby na internetu. Díky Memcached má Facebook rychlejší přístup k informacím. Důvodem je vytvoření cache

vrstvy mezi webovými servery a MySQL servery. Vytvořením této vrstvy se zrychlí přístup k databázi, který je obvykle pomalý. Stejně jako tomu bylo u balíčku LAMP, i u Memcached Facebook udělal nespočet optimalizací pro zlepšení výkonu. (9)

HipHop pro PHP

Hlavním cílem Facebooku je být rychlý a výkonný. K tomu slouží právě i HipHop, díky kterému se podařilo redukovat využití CPU na webových serverech Facebooku přibližně o 50%. HipHop funguje jako překladač kódu z PHP do vysoce optimalizovaného C++ kódu. (10)

Haystack

Haystack slouží jako sklad jakýchkoliv objektů, nicméně Facebook jej používá především jako výkonné uložiště fotografií, kterých je na Facebooku obrovské množství. Každá fotografie je uložena ve čtyřech různých rozlišeních. (10)

BigPipe

BigPipe je systém, který generuje webové stránky po takzvaných pagelets, což jsou jednotlivé části webové stránky. U úvodní stránky Facebooku to jsou části jako například chat, události, novinky s příspěvky a aplikace. Výhodou je menší chybovost, kdy při chybě například načtení chatu se zbytek pagelets načte v pořádku. Jednotlivé pagelets mohou být načteny zároveň v různých stádiích načtení. Za pomoci tohoto systému se stránky v jakémkoliv prohlížeči načtou rychleji. (10)

Cassandra

Apache Cassandra je distribuovaný systém pro práci s velkým množstvím dat, který je bezchybný. Jedná se o úložný systém z rodiny NoSQL, který Facebook využívá při hledání v doručených zprávách. Kromě Facebooku Cassandru používá i například Digg. (10)

Scribe

Scribe je logovací systém, který slouží Facebooku interně k mnoha účelům. Byl vytvořen pro rychlé zpracování přihlášení do Facebooku a pro automatické řízení nových přihlášení podle potřeby. Nových přihlášení tak mohou být stovky. (10)

Hadoop a Hive

Hadoop je implementace, která umožňuje provádět kalkulace na obrovském množství dat. Hive pochází přímo od Facebooku a lze pomocí něj zasílat SQL dotazy na Hadoop. Tím usnadňuje práci s Hadoop lidem bez větších programátorských zkušeností. (10)

Varnish

Varnish funguje jako http akcelerátor, který může fungovat jako load balancer, nebo cache obsahu, který je doručen uživateli velmi rychle. Facebook používá Varnish pro fotky a profilové obrázky a jako většina softwaru co Facebook používá je open source. (12)

Thrift

Facebook používá velké množství programovacích jazyků, jako například PHP, Java, C++ nebo Erlang pro chat. Thrift byl vyvinut jako rámec pro komunikaci mezi těmito jednotlivými jazyky. (10)

Gatekeeper

Facebook má dále systém Gatekeeper, který mu umožňuje spustit různý kód pro různé skupiny uživatelů. Toto umožňuje Facebooku lepší testování nových vlastností systému a například aktivaci nových funkcí, či služeb pouze pro zaměstnance Facebooku. Gatekeeper umožňuje také tzv. „dark launches“, což je spuštění určitého elementu, nebo funkce na pozadí tak, že si toho uživatel nevšimne. Toto slouží pro testování funkcí před oficiálním spuštěním. (10)

2.3.1.3 Vývoj Facebooku

4. 2. 2018 Facebook oslavil už čtrnácté výročí od vzniku. Facebook prošel mnoha změnami a dosáhl na několik historických milníků.

Okolo roku 2008 se Facebook dostal nad hranici 100 milionů uživatelů. Po celou svou dosavadní dobu, a ještě dalších asi pět let poté měl Facebook problém s penězi. Facebook tou dobou získával finance především z fondů rizikového kapitálu. V té době se předpovídalo, že klasickou reklamu nahradí lajky a sdílení uživatelů, co je potřeba si koupit, a Facebook potřeboval třetí firmy, který by tento nový "nereklamní reklamní" model prodávaly. Jako tyto třetí firmy, které Facebook potřeboval, vyrostly Socialbakers a Cambridge Analytica, které mohly jako základní nástroj využívat Facebookvé Graph API, které ve verzi 1.0 umožňovalo z profilů uživatelů a jejich přátel stáhnout téměř jakékoliv jejich informace. Nakonec ale Facebook skončil u klasického reklamního systému. (8)

V roce 2009 byl po nepokojích v Urumči Facebook zakázán v Číně. Podle The New York Times Facebook vyvinul software, který umožňuje blokovat zobrazování vybraných informací v určitých oblastech, který by měl pomoci firmě vrátit se na čínský trh, Facebook ale nezamýšlí používat software sám, ale plánuje ho nabízet k využívání jiným subjektům.

V roce 2010 společnost získala v soutěži Křišťálová Lupa 1. místo v kategorii sociální sítě. Další ocenění získala za službu Facebook Chat (5. místo v kategorii komunikační technologie) a za mobilní verzi svých stránek (3. místo v kategorii mobilní služby).

Rok 2012 byl pro Facebook důležitý, protože se mu podařilo získat sociální síť Instagram, kterou odkoupil v dubnu za 1 miliardu dolarů. V květnu téhož roku Facebook vstoupil na burzu. Posledním velkým milníkem roku 2012 bylo říjnové dosažení miliardy aktivních uživatelů.

V červenci roku 2013 používalo mobilní verzi Facebooku více než 100 milionů lidí a v srpnu Facebook spustil internet.org, který má za úkol zajistit přístup k internetu na celém světě.

Na přelomu ledna a února roku 2014 Facebook spustil iOS aplikaci Facebook Paper, což byla aplikace, která sloužila jako noviny, nebo magazín pro zařízení od firmy Apple. 4. 2. 2014 Facebook oslavil desáté výročí od založení a při té příležitosti nabídl uživatelům tzv. Lookback, což umožnilo uživateli prohlédnout si video automaticky vytvořené z příspěvků, které vložil za posledních 10 let. V únoru 2014 přišla ještě jedna důležitá událost pro Facebook, tou bylo odkoupení mobilní aplikace WhatsApp za 16 miliard dolarů. V březnu 2014 Facebook odkoupil další společnost, tentokrát Oculus VR, Inc., což je vedoucí společnost v oblasti virtuální reality. Mezi hlavní funkce, které byly spuštěny v roce 2014, patří Safety Check a Rooms.

V dubnu roku 2015 bylo v Messengeru umožněno uživatelům provádět videohovory. V červnu Facebook spustil tzv. Moments, což zachycuje momenty sdílené uživatelem na Facebooku s určitým přítelem. V srpnu 2015 bylo spuštěno live video pro veřejné příspěvky a koncem tohoto měsíce dosáhl Facebook dalšího velkého milníku, když oznámil, že v jeden den použila Facebook více než jedna miliarda lidí.

V polovině srpna 2017 spustil Facebook prodejní portál Marketplace nově v 17 zemích, v Evropě mj. v Česku, Maďarsku, Rakousku, Francii, Německu, a v Itálii. Několik měsíců

před spuštěním Marketplace v Česku zavedl Facebook možnost placení přes Messenger. Podle analytiků bylo důvodem zavedení těchto plateb získání většího přehledu o chování svých uživatelů.

V lednu 2018 vedení Facebooku oznámilo, že se chystá navýšit množství inzertního sdělení, při této příležitosti Mark Zuckerberg všechny ujistil, „že čas, který strávíme na Facebooku je dobře využitý“. Také začátkem roku 2018 Facebook vytvořil novou strategii zakazující reklamy na finanční produkty a služby jako binární opce, primární nabídky mincí a kryptoměny.

V únoru 2018 Facebook představil změny pravidel, které reagovaly na výhrady EU ohledně jeho zodpovědnosti za správu obsahu a požadavek sladit své uživatelské podmínky s evropskou právní úpravou o ochraně spotřebitelů. Podle Evropské komise, ale změny pravidel Facebooku řešily pouze částečně důležité otázky a nedostatky neodstraňovaly. (11) (12)

2.3.1.4 Facebook v ČR

V současné době (květen 2018) je v České republice asi 4,69 milionu registrovaných uživatelů Facebooku, což představuje skoro 45 % celé populace a skoro 65% internetově aktivního obyvatelstva. (13)

2.3.2 Twitter

Obrázek 1: Twitter. (Zdroj: www.twitter.com)

Twitter byl založen ve Spojených státech v San Franciscu v roce 2006. Dnes čítá přes 200 milionů uživatelů. Twitter je informační sociální síť, po které se šíří nejnovější informace v reálném čase. Uživatel si jednoduše najde to, co jej zajímá a o čem chce být informován. Twitter funguje za pomoci krátkých, max. 140 znaků krátkých zpráv, tzv. tweetů. Uživatelé mohou také sdílet odkazy a nahrávat videa či fotografie, které se ve tweetech zobrazí pouze jako internetový odkaz, který musejí uživatelé následně otevřít, aby se jim zobrazil obsah. Uživatelé tedy nevidí na hlavní stránce žádné obrázky ani videa, ale pouze

odkazy. Twitter také propojuje obchodníky s jejich zákazníky v reálném čase. Firmy s využitím Twitteru zveřejňují informace o produktech a službách, očekávají zpětnou vazbu od zákazníků či partnerů a vytvářejí si tak s nimi určitý vztah.

Výhodou Twitteru je možnost posílání tweetů pomocí sms, což také velice přispělo k jeho popularitě, ale bohužel sms tweety nejsou dostupné pro uživatele mobilních operátorů v České republice. Twitter je dostupný v 35 jazycích včetně češtiny. (14)

2.3.3 Youtube

Obrázek 2: YouTube: (Zdroj: www.youtube.com)

Jedničkou mezi video weby je bezesporu YouTube, který se dokázal prosadit ve velké konkurenci i bez podpory některého z portálů. YouTube byl založen v roce 2005 a v roce 2006 byl odkoupen společností Google za 1,65 mld. dolarů. První největší nárůst počtu měsíčních návštěv byl zaznamenán od ledna do června roku 2006, kdy se návštěvnost zvýšila ze 4,9 milionů na 19,6 milionů unikátních návštěvníků. Klíčem k úspěchu byla tolerance videí, která často poškozovala práva někoho jiného. Daly se zde najít hudební videoklipy a úryvky ze seriálů a filmů. V březnu 2007 YouTube kontroloval se 150 miliony přehráváními denně téměř polovinu trhu video serverů v USA. (15)

YouTube má v roce 2017 přes dvě miliardy přístupů denně a každou minutou uživatelé nahrají 300 hodin nových videí. YouTube je tak po internetovém vyhledávači Google druhou nejnavštěvovanější webovou službou světa. YouTube účet je zdarma a umožňuje uživateli nahrávat videa v několika různých formátech a můžete je nahrávat přímo z mobilního telefonu. Relativní novinkou je možnost nahrávání 3D videa a titulků. Videa jsou možná nahrávat ve vysokých rozlišeních (až 4K4), musí však být do maximální velikosti 2 GB a maximální délce 15 minut. Účet Vám umožňuje přidávat si přátele (psát jim zprávy), komentovat a hodnotit (líbí se X nelíbí se) oblíbená videa, sdílet videa na další sociální sítě (Facebook, Twitter, Myspace a další) a vytvářet si video seznamy. YouTube je dostupný v českém jazyce. (15)

2.3.4 Instagram

Obrázek 3: Instagram (Zdroj: www.instagram.com)

Další sociální sítí, která spadá pod společnost Facebook je Instagram. Tato aplikace vyšla 6. října 2010 a byla dostupná pouze pro platformu Apple, nyní je dostupná i pro platformy Android a Windows phone. Zakladatelem je Kevin Systrom, který na projektu spolupracoval s Mikem Kriegerem, kteří Instagram prodali společnosti Facebook v dubnu roku 2012 za miliardu dolarů. (17)

Hlavní funkcí Instagramu je sdílení fotografií a videí. Každý uživatel má možnost při přidání fotografie nebo videa využít jednoho z mnoha filtrů pro úpravu. Kromě filtrů má uživatel možnost upravit jas, kontrast, sytost, strukturu, barvu a další vlastnosti fotografie nebo videa, které se chystá nahrát. Na Instagramu bylo možné nahrávat fotografie a videa pouze ve čtvercovém formátu, to však od verze aplikace 7.5 neplatí a Instagram při nahrání multimédia

umožňuje uživateli vybrat mezi formátem krajina a portrét.

Dále Instagram nabízí možnost instalace funkcí Boomerang a Layout. První jmenovaná funkce umožňuje uživateli vytvářet a sdílet minividea. Díky funkci Layout může uživatel přidat více fotografií do jednoho příspěvku na Instagramu. V posledním kroku před zveřejněním obsahu uživatel může přidat místo, označit lidi a přidat popisek, ve kterém jsou často používány hashtagy. (18)

2.3.5 LinkedIn

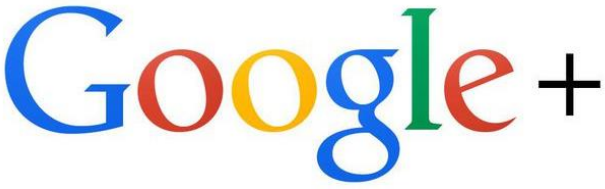
Obrázek 4: LinkedIn. (Zdroj: www.linkedin.com)

Sociální síť LinkedIn vznikla v roce 2003, o rok dříve než Facebook. LinkedIn, s více než 135 miliony uživateli, lze dnes považovat za největší profesní síť na světě. Nejvyšší popularitě se těší v USA, čím dál více získává popularitu ale i v České republice. Na síti působí nejčastěji manažeři, konzultanti a odborníci z různých oborů, nicméně jako stěžejní pracovní nástroj jej používají mnozí headhunteři a personalisté. Ti na profesní síti hledají prostřednictvím uživatelských životopisů vhodné kandidáty na pracovní místa, jelikož LinkedIn nabízí velké množství informací o potenciálních zaměstnancích. Kromě fyzických osob, podobně jako na Facebooku, působí na LinkedIn i firmy.

Růst uživatelské základny sítě LinkedIn lze označit za pomalý ale stabilně rostoucí. Pro představu, v říjnu roku 2009 dosáhl LinkedIn 50 milionů uživatelů, v dubnu 2018 jejich počet překročil 300 milionů.

Co se týče charakteristiky uživatelů, ze 44 % LinkedIn používají Američané, dále pak Indové, Brazilci, v Evropě pak Holanďané, Francouzi a Italové. Profesní síť používají spíše muži (61 %). Co se věku týče, 36 % uživatelů je ve věku 25-54 let, a 21 % ve věku 18-24 let. Z průmyslu jsou nejvíce zastoupeny firmy technologické (17 %), finanční (14 %), obchodní (12 %), výrobní (10 %), akademické (10 %), správní/administrativní (10 %). (19)

2.3.6 Google+



Obrázek 5: Google+ (Zdroj: www.google.com)

Další sociální sítí firmy Google je Google+. Tato sociální síť byla vytvořena jako konkurence pro Facebook, nicméně není tak úspěšná jako Facebook a nedosahuje ani

takové popularity jako druhá sociální síť společnosti Google YouTube. Funkčnost služby Google+ je v mnoha směrech stejná jako u Facebooku, pouze se určité funkce liší názvem nebo specifickou funkcionalitou. Mezi odlišnou funkcionalitu se dá považovat komunikace. Google+ totiž oproti Facebooku poskytuje komunikaci samostatně jako oddělenou službu nazvanou Hangouts, která poskytuje uživatelům komunikaci prostřednictvím textových zpráv, telefonního hovoru a videohovoru.

Velkou výhodou Google+ je propojení s ostatními službami a funkcemi společnosti Google. Přímo v panelu Google+ má uživatel možnost přejít na služby Hangouts, Gmail, Google Play, YouTube, Google Drive a mnoho dalších služeb, pro které se uživatel nemusí znovu přihlašovat. 43 Zásady ochrany osobních údajů jsou v tomto případě stejné jako u YouTube, proto je zbytečné je zde rozebírat znovu. (20)

2.4 České sociální sítě

Sociální sítě Facebook, Twitter, Myspace a další zahraniční sociální sítě jsou sice v popředí celosvětového zájmu, ale to neznamená, že by čeští uživatelé neměli možnost využívat i služby českých sociálních webů. S nárůstem uživatelů sociálních sítí, rostla i nabídka nejenom v zahraničních podmínkách. V ČR vznikaly sociální sítě ať už záměrně, či postupným vývojem, jako Lidé.cz, kdy se z komunikačního webu postupně stala plnohodnotná sociální síť. Mezi nejznámější a nejužívanější sociální sítě v ČR můžeme zahrnout Lidé, Líbímseti.cz, Spolužáci.cz, na které se následně podrobněji zaměříme.

2.4.1 Lidé.cz

Obrázek 6: Lidé.cz (Zdroj: www.lide.cz)

Sociální síť Lidé.cz patří mezi nejpopulárnější v České republice. Lidé.cz slouží také jako brána k dalším službám, jako jsou spolužáci, seznamka aj. Sdružuje jeho uživatele a nabízí jim možnost prezentování své osoby s dalšími připojenými projekty jako např. výuka jazyků aj.

Lide.cz, jedna z největších sociálních sítí, je provozována společností Seznam.cz. Vznik této sociální sítě se datuje do roku 1997, kdy byla spuštěna jako služba pro vyhledávání emailových adres. V roce 2004 společnost Seznam.cz kupuje majoritní podíl v projektu

Spolužáci.cz, přetváří jeho design a nasazuje ho jako další službu serveru Lidé.cz. V roce 2008 dochází k úpravě serveru Lide.cz, které je spojeno s větší zábavou pro uživatele – podpora videa, rozšíření fotogalerie, umožnění poslechu streamovaného hudebního rádia a výuku cizích jazyků.

Portál Lidé.cz najdeme na adrese http://www.lide.cz/ (viz. obr. 9) nebo také můžeme odkaz lidé.cz najít na serveru Seznam.cz. Lidé.cz je v podstatě vstupní brána, kde nalezneme nejenom profily uživatelů, ale také spousty odkazů na novinky a další popsané kategorie, které lze i bez registrace v omezenější formě prohlížet. Podobně, jako na síti Líbímseti.cz, můžeme po registraci posílat vzkazy dalším námi vybraným uživatelům.

Hlavní kategorie, které nalezneme na portálu Lidé.cz:

Chat – možnost psaní si v reálném čase se spoustou uživatelů; na výběr je obrovské množství kategorií a podkategorií-místností

Profily – v této části je možno vyhledat si uživatele, ať už náhodně nebo podle zadaných kritérií, jako je přezdívka, věk, pohlaví atd.

Diskuse – zde je možnost reagovat na příspěvky v daných tématech ať už náhodně; je zde možnost i založit vlastní téma diskuse

Videa – vlastní videa uživatelů sítě Lidé.cz.

Rádio – odkazy na nejrůznější on-line rádia rozdělené do přehledných kategorií, např. podle hudebního stylu

Seznamka – podobné jako profily, s tím rozdílem, že zde je možnost reagovat na skutečné inzeráty uživatelů; najdeme zde mimo jiné kategorie Vážná seznámení, Dopisování a přátelé, Cestujeme, Sport atd.

Srazy – nabídka nejrůznějších akcí seřazených podle kalendáře a místa, kde se bude konat, nejenom v ČR; nechybí možnost přidání vlastní akce

Blogy – nejrůznější články, nápady uživatelů

Hry – na výběr je velké množství her seřazeny do přehledných kategorií.

Spolužáci – odkaz na oblíbenou síť, kde lze vyhledat požadovanou školu či třídu (více o této síti bude v následující kapitole)

Výuka – jedna z posledních přidaných funkcí sítě Lidé.cz.; v odkazu Výuka lze najít nejenom kurzy jazykové, ale také kurzy výpočetní techniky, účetnictví, digitální fotografie; základní kurzy jsou zdarma, ale je pokud by chtěl uživatel rozšířit svoji výuku, lze si dokoupit i placené kurzy

Soutěže – soutěže o peněžité výhry, kterých se uživatelé mohou zúčastnit prostřednictvím zprávy SMS

Sociální síť Lidé.cz se v podstatě nijak zvlášť neodlišuje od svých konkurentů. Nabízí nám podobné a někdy i propracovanější funkce než ostatní sociální sítě podobného zaměření. Některé funkce mohou být více propracované a obsáhlé jako např. seznámení přes inzeráty, podobné inzerátům z tisku. (21)

2.4.2 Líbím se ti.cz

Obrázek 7: Líbímseti.cz (Zdroj: www.libimseti.cz)

Líbímseti.cz patří mezi největší komunitní a sociální sítě v České republice. Nalezneme zde mnoho služeb, funkcí a aplikací určených pro zábavu, chatování, sdílení a hodnocení fotografií atd. Tato sociální síť je především určena na službu seznamování se s ostatními uživateli a vzdáleně se podobá zahraniční sociální síti Myspace.

Začátky portálu Líbímseti.cz sahají až do roku 2002, který vznikl pro hodnocení fotek zaregistrovaných uživatelů. Přidáním neregistrovaných uživatelů v roce 2004, kteří se mohli také zúčastňovat hodnocení, se návštěvnost tohoto portálu velmi zvýšila. Během roku 2006 došlo ke grafické změně portálu, a především k přidání nových služeb.

Server a přihlášení do sítě Líbímseti.cz najdeme na adrese http://libimseti.cz/. I bez registrace do této sociální sítě je umožněno nahlížet na stránky jednotlivých uživatelů, kde nalezneme jejich profil s fotografiemi, informacemi o nich, příp. jejich zájmy a názory. Pokud bychom chtěli některého registrovaného uživatele kontaktovat např. napsat mu vzkaz či ho pozvat na chat, musíme se zaregistrovat.

Mezi další funkce tohoto severu patří:

Hodnoceni vzhledu uživatelů – na stupnici 1–10, lze vyjádřit svoje sympatie k uživatelům

Videochat – klasický chat obohacený možností sledování ostatních uživatelů prostřednictvím webové kamery

Vlastní internetové rádio – lze vybrat ze čtyř hudebních žánrů (pop, rock, dance a hip-hop)

Libimseti Life – pořádání seznamovacích akcí, což umožňuje uživatelům osobní seznámení

Hry – velký výběr online her, ať už proti živým soupeřům, nebo hry, které můžeme hrát sami, za zmínku stojí klasické hry jako např. šachy, prší, slovní fotbal

Magazín – články z různých kategorií – od módy až po horoskopy

Libimseti.cz se prezentuje jako zábavní server pro mladé lidi, kteří chtějí dát vědět ostatním nejen o své osobě. Je především zaměřen na službu seznamky s ostatními uživateli, takže člověk hledající seznámení, může zcela jistě navštívit tento server. (22)

2.4.3 Spolužáci.cz

Obrázek 8: Spolužáci.cz (Zdroj: www.goole.com)

Česká společnost Seznam.cz oznámila, že po 14 letech ukončuje provoz služby Spolužáci.cz. Jako důvod uvedla firma nízkou návštěvnost a obtížnou ochranu osobních údajů.

„Po 14 letech fungování zavírá společnost Seznam.cz svou Spolužáci. Ta bude v plné verzi fungovat do 24. května 2018“ uvedla Aneta Kapuciánová z firmy Seznam na oficiálním blogu. Poté bude omezen, až do konce srpna 2018 si však uživatelé budou moci stáhnout své fotografie a další data. Prvního září Spolužáci definitivně skončí.

Z blogu lze vyčíst dva hlavní důvody pro uzavření této služby. Prvním má být nízká návštěvnost kolem 20 tisíc lidí denně. „Pokles nových uživatelů jsme na Spolužácích začali pociťovat v roce 2015. Ačkoli měla služba původně sloužit zejména pro žáky a

studenty, používali ji spíše absolventi, kteří skrze ni udržovali vzájemné kontakty," vysvětluje Veronika Prokopová, produktová manažerka služby Spolužáci.cz.

Druhým důvodem je Obecné nařízení o ochraně osobních údajů (tzv. GDPR), které vejde v platnost na konci května 2018. „Abychom mohli změny, které z něj vyplývají, implementovat na Spolužácích, museli bychom službu od základů přepsat," uvedla Prokopová. To by podle ní bylo příliš náročné a drahé, proto se Seznam rozhodl provoz služby ukončit. Firma službu neplánuje nahradit.

Server Spolužáci.cz funguje od roku 1999, o pět let později jej koupil Seznam.cz. Ještě v roce 2009 patřil k nejoblíbenějším komunitním sítím v Česku s přibližně 1,5 milionem návštěvníků měsíčně. Překonala ho tehdy jen služba Lidé.cz, rovněž ze stáje Seznam.cz.

Lokální sociální sítě však byly už tehdy na ústupu. Válcoval je především Facebook, který postupně získal v Česku asi pět milionů uživatelů. Každý den na Facebook přistupuje 3,7 milionů Čechů. (23)

2.5 Obsah sociálních sítí

Obsah sociální je velmi různorodý. Proto, aby bylo možné definovat hrozby, je nutné vědět, kterých informací se mohou týkat. Níže jsou uvedeny informace, které sociální sítě mohou obsahovat:

- Osobní identifikační informace jak uživatele samotného, tak druhých osob – rodné číslo, jméno, příjmení, místo bydliště, vyznávané náboženství,
- Osobní citlivé informace jak uživatele samotného, tak druhých osob – zdravotní stav, fotografie, videa, zvukové záznamy,
- Autentizační údaje nebo informace, díky nimž lze autentizační údaje získat – hesla, jména domácích zvířat, příbuzných, spolužáků, kolegů,
- Informace, které prozrazují chování jak uživatele samotného, tak druhých osob – zvyky, způsob komunikace, koníčky, zaměstnání,
- Geografickou polohu jak uživatele samotného, tak druhých osob – aktuální polohu uživatele, místo a datum plánované dovolené, bydliště přátel a příbuzných, oblíbené restaurace;
- Pracovní informace – informace o struktuře organizace, pracovních kolezích, dodavatelích, zákaznících, plánech organizace, aktuálních projektech, pracovní dokumentace,

- Záznam komunikace – komunikace s rodinnými příslušníky, známými, kolegy z práce, zákazníky, dodavateli,
- Informace o majetku jak uživatele samotného, tak druhých osob – fotografie, videa, seznamy majetku.

2.6 Důvody pro získání informací ze sociálních sítí

Pro definování hrozeb a jejich pravděpodobnosti, je důležité identifikovat důvody, proč může dojít ke zneužití informací na sociálních či ke kompromitaci uživatelského účtu či identity. Mezi důvody patří:

- Odcizení majetku,
- Sledování chování uživatele nebo druhých osob,
- Sledování geografické polohy uživatele nebo druhých osob,
- Sledování komunikace uživatele nebo druhých osob,
- Získání citlivých/kompromitujících informací uživatele nebo druhých osob,
- Finanční motivace (prodej či zneužití identity/uživatelského účtu).

2.7 Rizika a hrozby sociálních sítí

Jelikož jsou sociální sítě rozšířené a hojně používané, věnují se jejich problematice v nemalé míře média. A právě média nejčastěji informují o jejich kompromitaci, neboť právě tyto informace představují pro senzacechtivé čtenáře lákavé téma. Většinou se totiž týká právě jich samotných nebo jejich nejbližších. Mohou se tak dozvědět zajímavé informace ze soukromí hvězd, souseda z protějšího bytu, známých či rodinných příslušníků. Média v tomto případě působí v rámci zveřejňování zmíněných příspěvků jak negativně, prostřednictvím zveřejnění leckdy citlivých informací, tak edukativně, kdy uživatele varují před hrozbami a doporučují bezpečné vzorce pro chování na sociálních sítích.

2.7.1 Příklady známých hrozeb

Níže jsou uvedeny příklady hrozeb a incidentů týkající se sociálních sítí, které byly prezentovány veřejně dostupných médiích.

2.7.1.1 Podvodníci útočí přes Facebook. Využívají zkopírovaný profil přátel

V poslední době se po Facebooku šíří nová vlna podvodů, která se snaží z neopatrných uživatelů vylákat peníze.

Se špatnou češtinou a podvrhnutým profilem se pokoušejí útočníci zneužít důvěřivost uživatelů a získat tak obnos ve výši mnoha set korun.

„*Jednou z variant je, že útočníci okopírují profil vybrané osoby a následně pošlou žádost o přátelství podle seznamu přátel. Oběti pak po přijetí obdrží zprávu s prosbou o telefonní číslo a následné přepsání kódu ze zaslané SMS zprávy. Zaslaný kód je od platební brány poskytovatele mobilních služeb oběti a potvrzuje platbu pohybující se kolem 1 300 až 1 400 korun. Útočník si následně kód vyžádá,“ popisuje scénář útoku národní bezpečnostní tým.*

Uživatele by měla odradit úroveň češtiny, kterou útočníci komunikují. CSIRT uvádí příklady: „hi dej mi své císlo?”, „nyní sms dorazila vodafone?”, „Vysvetlím Ti to. Napiš mi, prosím te, ten príchozí kód?”

Pokud se na takovou žádost nachytáte, doporučuje se neprodleně kontaktovat provozovatele platební brány a policii. (24)

2.7.1.2 Obří skandál Facebooku. Únik osobních údajů se mohl týkat dvou miliard lidí

Identita a další osobní údaje většiny z více než dvou miliard uživatelů Facebooku se mohly dostat do nepovolaných rukou. Na svém blogu to oznámila společnost Facebook, která stejnojmennou síť provozuje. Facebook doposud umožňoval hledat osoby podle e-mailu či telefonu, čehož mohli takzvaní sběrači dat zneužít. Tato funkce je od středy zablokována.

„Až do dneška lidé mohli zadat telefonní číslo či e-mail jiné osoby do vyhledávače Facebooku, což jim pomohlo je najít. Bylo to velmi praktické při hledání přátel v jazycích, ve kterých je komplikované vypsat celé jméno, nebo v případech, že lidé mají stejná jména,“ napsal ve středu na blogu technologický ředitel podniku Mike Schroepfer. Dodal ale, že tuto funkci k získání dat z veřejné části profilů mohli zneužít sběrači dat.

Sběrači dat díky e-mailovým adresám a telefonním číslům, které si mezi sebou hackeři vyměňují či které jsou na internetu dostupné, mohli pomocí zmíněné aplikace Facebooku získat jména osob a další osobní informace, jako jsou místo bydliště či zaměstnání. Vždy ovšem záleželo na tom, jaké údaje o sobě konkrétní uživatel na veřejné části profilu uvedl. „*Vzhledem k rozsahu a propracovanosti aktivity, kterou jsme zaznamenali, si myslíme, že veřejné profily většiny uživatelů Facebooku mohly být takto prozkoumány,“* uvedl Schroepfer.

Aféra vypukla kolem sběru dat společností Cambridge Analytica. Ta čelí obviněním, že získané údaje o uživatelích Facebooku využívala k ovlivňování voleb. Data údajně sloužila mimo jiné k vývoji softwarových nástrojů pro podporu volební kampaně Donalda Trumpa v roce 2018. (25)

2.7.1.3 Přes Facebook Messenger se šíří kód, který tajně těží kryptoměnu

Kombinace Facebook Messengeru a prohlížeče Google Chrome, přes který je spuštěn, může vést ke spuštění kódu, který tajně na počítačích oběti těží kryptoměnu Monero.

Antivirová firma Trend Micro, která problém popisuje, uvádí, že se závadný kód, označovaný jako Digimine, začal šířit nejdříve v Jižní Koreji. Později se automatický těžař začal šířit do Vietnamu, Ázerbájdžánu, Ukrajiny, Filipín, Thajska, Venezuely a dalších zemí.

Současná verze těžebního robota Digmine funguje pouze na klasickém počítači, takže mobilní uživatelé nejsou zasaženi. Malware se šíří jako soubor videa, ale je to spustitelný skript na psaný v AutoIt, který na počítačích oběti začne těžit.

Šíří se tak, že přihlásí na messengerový účet uživatele, pokud má nastavené automatické přihlášení. Poté se rozešle na všechny přátele z Facebooku s odkazem na falešné video.

Automaty, které na počítačích oběti tajně těží kryptoměny, se stávají stále populárnější, jak cena digitálních měn roste. Využívají je nejen útočníci, ale i některé webové stránky, které si tak chtějí přivydělat. (26)

2.7.1.4 Prozrazení komunikace

Při soukromém chatu na sociálních sítích uživatel předpokládá, že komunikaci může sledovat pouze on a protistrana, se kterou komunikuje. Realita je však taková, že chatová komunikace je poskytovatelem chatovací služby sledována a analyzována. Upozorňuje na to například článek renomované agentury Reuters (Social networks scan for sexual predators, with uneven results), který poukazuje na příznaky chování takového charakteru. V rámci analýzy obsahu chatu jsou stroji sledovány například používané slovní výrazy a věk komunikujících stran. Pokud stroj vyhodnotí, že komunikace prostřednictvím chatu jeví známky podezřelého chování, například sexuálního, je automaticky upozorněna příslušná osoba na straně provozovatele soc. sítě. Ta podezřelou komunikaci detailněji přešetří a případně podnikne další kroky.

Zaměstnanci, pověřené osoby a třetí strany, které dostanou oprávnění od provozovatele sociálních sítí nahlížet do chatu na sociálních sítích, mohou s takovými informacemi dále nakládat a zneužít je. Zdání, že chat je zcela privátní, je klamný. (27)

2.7.1.5 Falešné profily

Na sociálních sítích se vyskytuje nepočitatelné množství uživatelských profilů, které se vydávají za populární osobnosti či vizuálně zajímavé lidi. Ve skutečnosti se však jedná o falešné uživatelské profily, které se skutečnými uživateli nemají nic společného. Jejich cílem je kompromitovat potencionální oběti.

Útočník, který se za podvrženou identitou skrývá, se pokouší posílat uživateli zprávy, obrázky, soubory obsahující nebezpečný malware. Následně, prostřednictvím malwaru odcizit hesla, či číst e-mailovou a jinou digitální komunikaci, ovládnout uživatelský profil, účet či celý operační systém a počítač. Útočník, tedy uživatel falešného identity může též použít techniky sociálního inženýrství. S ukradenými profily se obchoduje například na http://www.buyaccountsnow.com/. Ceny ukradených uživatelských profilů se pohybují kolem cca za 6 centů za účet, u účtů s ověřeným fyzickým uživatelem, je cena kolem 1,5 dolaru. (28)

2.7.2 Seznam hrozeb

V této kapitole jsou sepsány hrozby, které ohrožují sociální sítě. Seznam hrozeb je čerpán z veřejně dostupných zdrojů, které o incidentech spojených se sociálními sítěmi informují, dále z praktických zkušeností uživatelů popisovaného podniku. Seznam hrozeb je dále použit pro výpočet velikosti rizik v kapitole Analýza rizik.

Tabulka 1: Seznam hrozeb sociálních sítí (Zdroj: Vlastní zpracování)

Název hrozby	Popis hrozby
Falšování identity	Podvržení uživatelské identity. Pachatel vytvoří na sociální síti uživatelský účet pod falešnou identitou, v rámci které na sociální síti dále vystupuje. V rámci falešné identity získává od ostatních uživatelů (přátelé, členové rodiny) citlivé informace, které pak dále zneužívá (např. prodej, loupež, vydírání,

	poškozování reputace), či páchá činy ve jménu podvržené identity. Jeho pravá identita zůstává skryta. Pokud se jedná o podvržení reálné identity, mohou být škody provedené v rámci falešné identity, vymáhány po identitě reálné.
Odcizení identity	Uživatelovi je odcizena identita, kterou si sám na sociální síti vytvořil. Pachatel zpravidla získá uživatelovy autentizační údaje k uživatelskému účtu, prostřednictvím kterých se následně identity zmocní. Původní majitel se o odcizení dozví většinou podle toho, že se ke své identitě nepřihlásí, jelikož pachatel změnil přístupové údaje. Pokud pachatel přístupové údaje nezmění, dá se předpokládat, že pokud uživatel nekontroluje informace o přístupu k uživatelskému účtu, tak odcizení přístupových údajů vůbec nezjistí. Díky odcizení uživatelské identity může pachatel zneužít veškeré informace, které obsahuje profil odcizené virtuální identity či páchat činnost v rámci odcizené identity. Možné důsledky z páchané činnosti odcizené identity by ale v tomto případě mohl nést reálný vlastník odcizené identity.
Prozrazení aktuální polohy uživatele samotným uživatelem	Pomocí geolokační služby mohou uživatelé sdílet s ostatními uživateli informace o poloze, kde se právě nachází. Na základě informace o poloze uživatele, může pachatel například v jeho nepřítomnosti vykrást jeho byt či páchat jinou trestnou činnost.
Prozrazení aktuální polohy uživatele jeho přáteli	Pomocí geolokační služby mohou přátelé uživatele uvádět na sociální síti informace jeho o poloze a sdílet ji s ostatními uživateli. Na základě informace o poloze uživatele, může pachatel například v jeho nepřítomnosti vykrást jeho byt či páchat jinou trestnou činnost.
Šíření malwaru	Sociální sítě mohou být zneužity pro šíření malwaru. Malware se šíří sociálními sítěmi několik způsoby: • prostřednictvím vložených odkazů ve sdílených příspěvcích uživatelů. Odkazy, které se tváří jako odkaz

	na zajímavý obsah, vedou ke stažení malwaru, či na webové stránky nakažené malwarem. • prostřednictvím aplikací a her, které jsou ve skutečnosti malwarem, nebo malware stahují. Prostřednictvím malwaru mohou útočníci získat citlivé informace uživatelů včetně autentizačních údajů ke službám, bankovním účtům apod.
Vědomé zveřejnění citlivých informací samotným uživatelem	Uživatel zveřejní citlivé informaci na sociální sítě, aniž by tušil možný negativní dopad jejich zveřejnění. Jedná se například o aktuálně vložené fotky z dovolené z druhé strany planety vzdálené stovky kilometrů od jeho bydliště. Pokud takovou informaci zločinec zjistí, může to být návodná informace proto, aby šel oběti vyloupit dům.
Únik citlivých informací prostřednictvím chyby uživatele	Uživatel sociální sítě chybně nastaví, ať už z nedbalosti či z neznalosti, přístupová oprávnění pro sdílené citlivé informace. Jedná se například o zveřejnění intimních fotografií, videí apod.
Únik citlivých informací prostřednictvím chyby provozovatele sociální sítě	Provozovatel sociální sítě chybně nastaví/nedostatečně zabezpečí algoritmus přístupových oprávnění pro sdílené citlivé informace. Pro útočníka je pak snadné se k citlivým informacím dostat a dále je zneužít. Jedná se například o zveřejnění citlivých informací z důvodu změny přístupových práv sociální sítě.
Únik citlivých informací prostřednictvím chyby třetí strany	Prozrazení informací třetí stranou. Uživatel, se kterým sdílíte citlivé informace, chybně nastaví, ať už z nedbalosti nebo z nevědomosti, přístupová oprávnění pro sdílené informace. Pokud útočník nenajde citlivé informace na vašem profilu, může je najít na profilu vašich přátel.
Sdílení přístupových údajů	Autentizační údaje pro přístup k účtu virtuální identity na sociální síti sdílí více fyzických lidí. Vyšší pravděpodobnost

	úniku citlivých údajů, nemožnost identifikovat konkrétní odpovědnou osobu za provedené činy.
Sledování chování uživatele	Provozovatelé sociální sítí či třetí strany mapují chování uživatele (jaké má koníčky, přátele, zaměstnání, záliby, vztahy, bydliště, lokální umístění, požívané prostředky, vlastněná aktiva, používané služby atp.). Získané informace ze sledovávání mohou použít ve svůj prospěch či například prodat marketingovým společnostem či jiným stranám, kteří mohou informace dále zneužít.
Nedostatečné zabezpečení sociální sítě	Provozovatel sítě má nedostatečně zabezpečenou architekturu a fungování sociální sítě, například slabý autentizační mechanismus nebo nedostatečně zabezpečené (zašifrované) autentizační údaje (jméno, heslo). Při úniku autentizačních údajů hrozí odcizení identity a únik/zneužití citlivých údajů dané identity. Při použití stejných autentizačních údajů u dalších služeb, aplikací, systémů atp., hrozí odcizení informací i z těchto aktiv.
Vymazání části komunikace	Uživatel zpětně vymaže část komunikace, což pozmění význam vět/komunikace.
Prozrazení organizační/rodinné struktury	Zmapování potenciálních cílů pro získání informací či případný útok. Zneužití sociálních vazeb prostřednictvím sociálního inženýrství.
Výpadek služby sociální sítě	Nemožnost používat sociální síť nebo její služby z důvodu výpadku sociální sítě.
Ztráta informací	Trvalá ztráta informací uložených na sociální síti.
Ztráta kontroly nad obsahem vloženým na sociální síti	Uživatel ztratí kontrolu nad obsahem uloženým v sociální síti například díky ztrátě autentizačních údajů.
Narušení	Sociální sítě nejsou obsaženy v bezpečnostních

bezpečností strategie/bezpečnosti firmy	pravidlech/politikách organizace. Organizace nemá zmapované hrozby, které hrozí z prostředí sociálních sítí a tedy nemá pokryta ani případná rizika.
Nedostatečná dokumentace	Nedostatečně dokumentované funkce sociální sítě. Uživatel se z nápovědy nedozní, jak nástroje sociální sítě pracují, či kde může provést potřebná nastavení. Důsledkem může být například prozrazení citlivých informací.
Ztráta/odcizení zařízení s přístupem na sociální sítě	Zařízení (PC, notebook, tablet, smartphone atp.) přihlášené k uživatelskému účtu (s autentizačními údaji) sociální sítě je ztraceno anebo odcizeno.
Ponechání bez dozoru zařízení s přístupem na sociální sítě	Zařízení PC, notebook, tablet, smartphone atp.) přihlášené k uživatelskému účtu (s autentizačními údaji) sociální sítě je ponecháno bez dozoru.
Uzamčení/zrušení účtu na sociální síti	Uživatelský účet na sociální síti je zrušen či uzamčen. Např. na základě porušení pravidel sociální sítě.

3 VLASTNÍ NÁVRH ŘEŠENÍ A IMPLEMENTACE

V následujících řádcích bude představena společnost, která bude předmětem analýzy rizik a hrozeb. Jak již bylo uvedeno v úvodu práce, firma si nepřeje zveřejnit svůj název a požaduje zachování anonymity. Představení bude proto provedeno spíše obecně a nebudou uvedeny údaje, které by mohly pomoct podnik identifikovat.

Praktická část je vypracována na základě interních zdrojů společnosti a informací získaných z rozhovorů a spolupráce s manažerem a zaměstnanci popisované firmy.

3.1 Představení společnosti

Popisovaná společnost působí na českém trhu již od roku 2006. Podnik působí jako distributor IT řešení pro domácnost i firmy. V rámci zakázek je tedy schopna realizovat na míru softwarové produkty vybavení jak malých, tak středě velkých a mezinárodních firem. Podnik si zakládá na kvalitním zpracování zakázek, udávání moderních trendů a na poskytování zákaznických služeb v průběhu a po realizaci zakázky.

Hlavním místem působnosti podniku jsou trhy na území České republiky a Slovenska. Samozřejmě však podnik hledá potenciální zákazníky i po celé Evropě, protože omezením se pouze na uvedené trhy by firma přicházela o případný další zisk.

3.1.1 Organizační struktura společnosti

Společnost zaměstnává 23 zaměstnanců na plný úvazek. Tito zaměstnanci se dělí do několika oddělení.

V čele společnosti stojí ředitel, který je zodpovědný na řízení, chod a výsledky společnosti a stanovení a plnění business plánu. Dále je za jednání s výrobci a reprezentaci firmy. Také zodpovídá za řízení, motivaci, podporu a výsledky podřízených zaměstnanců (obchodní ředitel, technický ředitel, finanční ředitel, manažer marketingu).

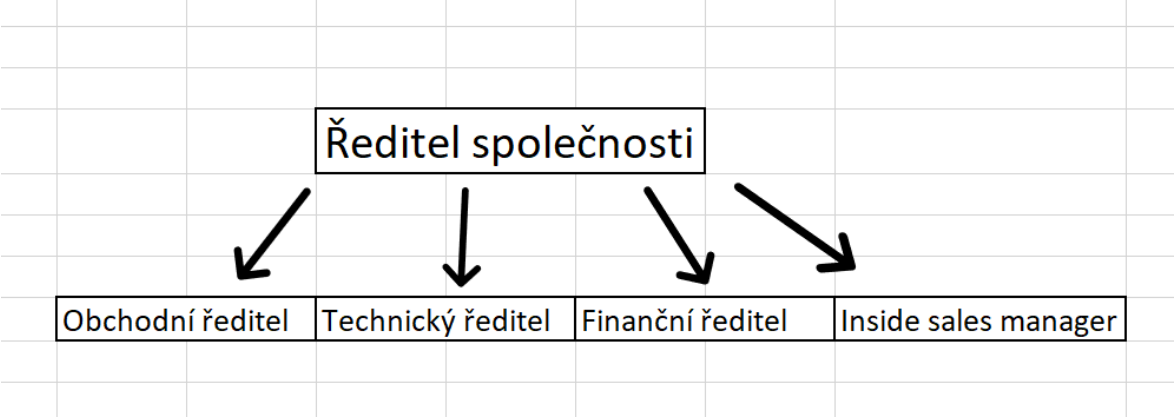
Obchodní ředitel je zodpovědný plnění obchodního cíle a výsledky obchodního oddělení. Řídí, motivuje a podporuje obchodní oddělení. Také je odpovědný za reprezentaci společnosti při vytváření a udržování obchodních vztahů a jednání s partnery.

Technický ředitel řídí činnosti technického oddělení (podpora, implementace, presales) a odpovídá za jejich plnění. Také je zodpovědný za správnou součinnost s ostatními odděleními a za technickou produktovou agendu jednání s výrobci.

Mezi další členy managementu patří finanční ředitel, ten je zodpovědný především za fakturaci, controlling, za pravidelný finanční reporting, řízení cashflow, za řádnou platební morálku k dodavatelům a řádný odvod všech typů daní ve správné výši.

Poslední člen managmentu je tzv. „delivery and inside sales manager“, ten vede tým „inside sales, což je interní podpora obchodního oddělení, delivery a produkt marketingu. Zodpovídá za jednání s výrobci o partnerském programu a podmínkách. Zodpovídá za běžnou agendu jednání s výrobci, za správnost a objednávek u výrobců a za reklamace.

Organizační struktura managementu podniku je zobrazena na následujícím obrázku (Obrázek 9).



Obrázek 9: Organizační struktura (Zdroj: Vlastní zpracování)

3.1.2 Sociální sítě ve společnosti

Po rozvorech se zaměstnanci společnosti jsem zjistil, že téměř všichni ve firmě používají buďto sociální sít Facebook, anebo sociální síť LinkedIn. Někteří z zaměstnanců a vedení uvedli, že mají profil na obou těchto sítích a pravidelně je používají i v pracovní době.

3.2 Analýza rizik

V této části práce bude provedena analýza rizik při používání sociální sítě v popsané společnosti a na základě jejich výsledků navrhnu opatření, která budou snižovat dopad na organizaci a/nebo pravděpodobnost výskytu rizika.

Hodnocení dopadů je provedeno pomocí vodítek, prostřednictvím kterých se převádí kvalitativní hodnoty na kvantitativní viz tabulky Číselné škály níže. Vodítka byla vytvořena na základě příkladů z normy *ISO/IEC 27035, Information technology — Security techniques — Information security incident management. (29)*

Aby se dalo provést ohodnocení aktiv, je nutné nejprve rizika ohodnotit. Tabulka 2 Stanovuje číselnou škálu pro pravděpodobnost výskytu hrozeb ve společnosti. V tabulce 3 uvedené níže jsem nejprve stanovil stupnici ohodnocení velikost dopadu hrozeb. V tabulce 4 jsou číselně ohodnocena pravděpodobnost úspěšné hrozby. Tyto tabulky poslouží jako základ pro analýzu rizik.

Tabulka 2 Stanovení číselné škály pravděpodobnosti výskytu hrozeb (Zdroj: Vlastní zpracování)

Číselné škály pravděpodobnosti výskytu hrozeb	**Pravděpodobnost**	**Popis**
1	Velmi nízká	Velmi nepravděpodobné, že se hrozba vyskytne. Ještě se nestalo.
2	Nízká	Nepravděpodobné, že se hrozba vyskytne. Stalo se výjimečně.
3	Střední	Pravděpodobné, že se hrozby vyskytne. Občas se stane.
4	Vysoká	Velmi pravděpodobné, že se hrozba vyskytne. Stává se často.
5	Velmi vysoká	Vysoce pravděpodobné, že se hrozba vyskytne. Stává se velmi často

Tabulka 3 Stanovení velikosti dopadu hrozeb (Zdroj: Vlastní zpracování)

Číselné škály pro hodnocení velikosti dopadu hrozeb	**Velikost rizika**	**Hodnocení dopadů**
1	Bezvýznamné riziko	Žádný dopad na firmu
2	Akceptovatelné riziko	Zanedbatelný dopad na firmu
3	Mírné riziko	Potíže či finanční ztráty

4	Nežádoucí riziko	Vážné potíže či podstatné fin. Ztráty
5	Nepřijatelné riziko	Existenční potíže

Tabulka 4 Stanovení číselné škály pravděpodobnosti úspěšnosti hrozeb (Zdroj: Vlastní zpracování)

Vodítka pro pravděpodobnosti úspěchu hrozeb	**Pravděpodobnost**	**Popis**
1	Velmi nízká	Velmi nepravděpodobné, že hrozba uspěje. Ještě se nestalo.
2	Nízká	Nepravděpodobné, že hrozba spěje. Stalo se výjimečně.
3	Střední	Pravděpodobné, že hrozba uspěje. Občas se stane.
4	Vysoká	Velmi pravděpodobné, že hrozba uspěje. Stává se často.
5	Velmi vysoká	Vysoce pravděpodobné, že hrozba uspěje. Stává se velmi často

Výpočet rizik je proveden podle modifikované metodiky, která vychází z normy *ČSN ISO/IEC 27005, přílohy E. 2.2 Příklad 2 Třídění hrozeb pomocí míry rizika*. (30)

Princip výpočtu míry rizika a seřazení hrozeb je zobrazeno v tabulce níže. Jednotlivé sloupce jsou pro lepší orientaci označeny písmeny. Data v jednotlivých sloupcích znamenají:

a) Název hrozby, která je hodnocena. Názvy hrozeb jsou čerpány ze *Seznamu hrozeb* z kapitoly 2.7.2.

b) Velikost dopadu (škála 1-5) při uskutečnění hrozby. Stanovuje se na základě vodítek z *Tabulka 3 Stanovení velikosti dopadu hrozeb.* Číselná velikost dopadu se určuje na základě scénáře (vodítka), který je k dané velikosti dopadu přiřazen.

c) Pravděpodobnost výskytu hrozby (škála 1-5). Stanovuje se na základě vodítek z *Tabulka 2 Stanovení číselné škály pravděpodobnosti výskytu hrozeb.*

Pravděpodobnost výskytu hrozby se vyjadřuje číselně na základě scénáře, který je k danému číslu číselné škály přiřazen.

d) Pravděpodobnost úspěchu hrozby (škála 1-5). Stanovuje se na základě vodítek z *Tabulka 4 Stanovení číselné škály pravděpodobnosti úspěšnosti hrozeb*. Pravděpodobnost úspěšnosti hrozby se vyjadřuje číselně na základě scénáře, který je k danému číslu číselné škály přiřazen.

e) Velikost míry rizika je vypočítávána vynásobením sloupce *b, c, d,* tedy hodnotami Velikosti dopadu, Pravděpodobnosti výskytu a Pravděpodobnosti úspěšnosti hrozby popsanými výše;

f) Ve sloupci „e“ jsou pak hrozby seřazeny sestupně dle vypočtené velikosti rizik. Čím je větší velikost rizika, tím má nižší pořadové číslo.

Prostřednictvím této metodiky jsou seřazeny hrozby s rozdílnými dopady, pravděpodobností výskytu a úspěchu dle míry rizik.

Tabulka 5 Příklad výpočtu rizik a jejich hrozeb dle velikosti rizik

(Zdroj: Vlastní zpracování)

(a)	(b)	(c)	(d)	(e)	(f)
Popis hrozby	**Velikost dopadu**	**Pravděpodobnost výskytu hrozby**	**Pravděpodobnost úspěchu hrozby**	**Velikost rizika b × c × d = e**	**Seřazení hrozeb**
Hrozba A	5	2	4	**40**	2-3
Hrozba B	2	4	3	**24**	4
Hrozba C	3	5	4	**60**	1
Hrozba D	1	3	2	**6**	6
Hrozba E	4	1	3	**12**	5
Hrozba F	2	4	5	**40**	2-3

Pro větší přehlednost velikostí rizik, jsou rizika rozdělena do barevné pětistupňové škály. Barevné označení jednotlivých rizikových skupin znamená:

Tabulka 6 Pětistupňová škála pro určování velikosti rizik (Zdroj: Vlastní zpracování)

Stupeň rizika	Popis velikosti rizika	Vypočtená velikost míry rizika
5	Velmi vysoké riziko	50-60
4	Vysoké riziko	30-40
3	Střední	20-30
2	Malé riziko	10-20
1	Velmi malé riziko	0-10

Níže je uveden výpočet velikosti rizik pro hrozby sociálních sítí uvedené v kapitole Seznam hrozeb

Tabulka 7 Výpočet velikosti rizik sociálních sítí (Zdroj: Vlastní zpracování)

Výpočet rizik					
Název hrozby	**Velikost dopadu**	**Pravděpodobnost výskytu hrozby**	**Pravděpodobnost úspěchu hrozby**	**Velikost rizika**	**Seřazení hrozeb**
Falšování identity	3	4	3	**36**	1-2
Sledování chování uživatele	3	4	3	**36**	1-2
Šíření nepravdivých informací, vyvolání paniky	4	4	2	**32**	3
Šíření malwaru	3	3	3	**27**	4
Sledování chování lidí	3	3	2	**18**	5-9
Únik citlivých informací prostřednictvím chyby třetí strany	3	3	2	**18**	5-9
Narušení bezpečností strategie/bezpečnosti firmy	3	3	2	**18**	5-9

Výpočet rizik					
Název hrozby	**Velikost dopadu**	**Pravděpodobnost výskytu hrozby**	**Pravděpodobnost úspěchu hrozby**	**Velikost rizika**	**Seřazení hrozeb**
Vědomé zveřejnění vlastních citlivých informací samotným uživatelem	3	3	2	**18**	5-9
Prozrazení aktuální polohy uživatele jeho přáteli	3	3	2	**18**	5-9
Prolomení/nedostatečné zabezpečení sociální sítě	4	2	2	**16**	10-12
Ztráta/odcizení zařízení s přístupem na sociální sítě	4	2	2	**16**	10-12
Odcizení identity	4	2	2	**16**	10-12
Změna možností nastavení uživatelského účtu	2	3	2	**12**	13-17
Únik citlivých informací prostřednictvím chyby uživatele	3	2	2	**12**	13-17
Sdílení přístupových údajů	3	2	2	**12**	13-17
Prozrazení aktuální polohy uživatele samotným uživatelem	3	2	2	**12**	13-17
Manipulace uživatelem	3	2	2	**12**	13-17
Ponechání bez dozoru zařízení s přístupem na sociální sítě	2	2	2	**8**	18-21
Ztráta kontroly nad obsahem	2	2	2	**8**	18-21
Uzamčení/zrušení účtu na sociální síti	2	2	2	**8**	18-21
Změna pravidel provozovatele sociální sítě	2	2	2	**8**	18-21
Prozrazení	1	3	2	**6**	22

Výpočet rizik					
Název hrozby	**Velikost dopadu**	**Pravděpodobnost výskytu hrozby**	**Pravděpodobnost úspěchu hrozby**	**Velikost rizika**	**Seřazení hrozeb**
organizační/rodinné struktury					
Vymazání části komunikace	1	2	2	**4**	23
Únik citlivých informací prostřednictvím chyby provozovatele sociální sítě	3	1	1	**3**	24

3.3 Zhodnocení rizik

Tato kapitola zahrnuje hodnocení výsledků analýzy rizik z kapitoly předchozí. Dále pak rozebírá možné dopady hrozeb, pokud by se jejich realizace naplnila. Dává výčet prvků, které vedou k motivaci bezpečného chování, a poskytuje pohled do budoucnosti bezpečnosti sociálních sítí.

3.3.1 Zhodnocení výsledků analýzy rizik

Z výše uvedeného hodnocení rizik viz *Tabulka 7 Výpočet velikosti rizik sociální sítí*, vyplývá, že třemi největšími riziky sociálních sítí jsou Falšování identity, Sledování chování uživatele a Šíření nepravdivých informací, vyvolání paniky. S ohledem na velikost vypočtených rizik zmíněná tři rizika spadají do kategorie Vysokých rizik viz *Tabulka 6 Pětistupňová škála pro určování velikosti rizik*. Kromě třech zmíněných Vysokých rizik, které přesáhly hranici 30 bodů v parametru *Velikost rizika*, je třeba zmínit ještě riziko, které dosáhlo 27 bodů. Na základě dosaženého hodnocení bylo riziko Šíření malwaru hodnoceno jako Střední riziko. Ostatní rizika nepřesáhla hranici 20 bodů, tedy jsou hodnocena jako Malá či Velmi malá rizika. Níže jsou podrobněji rozebrána čtyři největší rizika.

Vysoké riziko	Falšování identity

Vysoké riziko falšování identity vyplývá z četnosti výskytu dané hrozby, která je na sociálních sítích celkem častá. Falešné identity se týkají zejména známých osobností, u kterých lze najít na sociálních sítích i několik uživatelských účtů, ale většinou všechny jsou falešné. Nicméně, není vyloučeno, že potenciální útočník cíleně vytvoří falešnou identitu například vašeho blízkého známého, kterého najde ve vašem profilu na sociální síti v „Přátelích“. Po vytvoření falešné identity vašeho blízkého již útočníkovi stačí vás kontaktovat s tím, že je dotyčná „falešná osoba“, jen si vytvořila nový uživatelský profil a pokud dotyčná oběť nerozená falešnou identitu, může začít útočník „dolovat“ z oběti citlivé informace, které pak následně může zneužít ve svůj prospěch.

Ověření pravosti identity se může zdát na jednu stranu jednoduché, například díky odkazu z oficiálních stránek uživatele. Nicméně i webové stránky lze podvrhnout falešnými a oficiální stránky je možno hacknout a vložit na ně odkaz na falešnou identitu v sociální síti.

Za efektivní způsob ověření identity lze doporučit použití jiného informačního kanálu. Ideálně prostřednictvím osobního kontaktu, telefonicky, ověřeným emailem, videohovorem či doporučením/zaručením od důvěryhodné osoby.

Vysoké riziko	Sledování chování uživatele

Díky informacím, které uživatelé na sociální sítě dávají, lze snadno sledovat jejich chování a na základě pozorování pak lehce sestavit vzorec charakteristického chování, který lze použít například k vytvoření důvěryhodné falešné identity. Sledováním chování uživatele lze dále například vysledovat uživatelovi zvyklosti, koníčky, přátele, zdravotní stav a na základě těchto informací s dotyčným dále manipulovat. Například nabízet cíleně reklamu, vytvářet „řízené náhody“ atp. Sledování uživatele mohou provádět i samotní provozovatelé sociálních sítí tak jiné smluvní strany. Na základě získaných informací pak mohou zkoušet ovlivnit uživatele, jeho chování či rozhodování, například při koupi nového produktu. Získané informace též mohou prodat třetím stranám, které mohou informace dále využít ve svůj prospěch.

Obranou proti sledování je nepublikování osobních informací na sociálních sítích, či používání bezpečného módu webového prohlížeče při surfování internetem. Vyhnutí tomuto riziku je nepoužívání sociálních sítí.

Vysoké riziko	**Šíření nepravdivých informací, vyvolání paniky**

Riziko Šíření nepravdivých informací, vyvolání paniky vyplývá z vysoké četnosti nepravdivých zpráv, které na sociálních sítích kolují. Jejich nepravdivost se mnohdy složitě odhaluje. V případě důvěryhodně napsané podvodné zprávy, může být zmanipulována, díky rychlému sdílené informací prostřednictvím sociálních sítí, velká masa lidí. V důsledku zprávy je možné, že by vypukla panika velkého rozsahu, která by mohla způsobit velký dopad, případně i ztráty na životech.

Šíření nepravdivých informací lze předejít jejich ověřováním z více zdrojů. Například z denního tisku, důvěryhodných zpravodajských webů. Při ověřování je však nutné ověřovat původní zdroj zprávy, jelikož mnohé informace dnešní „novináři“ přebírají právě ze sociálních sítí. Pro získání důvěryhodné informace je nejlepší kontaktovat přímo toho, koho se zpráva týká, tedy konkrétní společnost, organizaci, člověka, například zákaznickou linku, help-linku, oddělení pro styk s veřejností či konkrétní dotčenou osobu.

Střední riziko	**Šíření malwaru**

Pro šíření malwaru jsou sociální sítě „populární platformou“. Jelikož uživatelé sociálních mezi sebou sdílí velký objem mediálního obsahu, je velice jednoduché vytvořit stránku se zábavnou tématikou, jejíž obsah budou během pár dnů odebírat stovky uživatelů. Pak již pouze stačí do jednoho příspěvku zařadit odkaz na webovou stránku, která obsahuje nebezpečný kód případně i instalátor zranitelné aplikace (hra, ovladač, mediaplayer), a infikovaní uživatelé jsou na světě. Do infikovaného zařízení už je pak pro útočníka hračkou zanést například keyloger (aplikace pro sledování a odesílání stisků kláves zařízení) a odcizit autentizační údaje například do internetového bankovnictví. Jelikož útočnici jsou stále vynalézavější, malware maskují například do her či „pseudo nových“ funkcí sociální sítí.

Obranou proti tomuto riziku je instalace antimalwarového řešení, otevírání pouze důvěryhodných odkazů či obecné vzdělávání ohledně nových hrozeb na sociálních sítích.

3.3.2 Možné dopady hrozeb

Hrozby, uvedené v kapitole Seznam hrozeb, mohou mít ve svém důsledku na uživatele a pro firmu různý dopad. Typy dopadů, které s hrozbami mohou souviset, jsou:

Finanční

- odcizení peněz z bankovního účtu – prozrazení autentizačních údajů (hesla) nebo údajů pro resetování autentizačních údajů (typicky např. jméno domácího mazlíčka/oblíbeného učitele/jméno matky za svobodna atp.);
- sankce od úřadů/firem na základě prozrazení tajných/citlivých – prozrazení citlivých informací jako jsou rodná čísla klientů, obchodní tajemství.

Hmotný

- odcizení majetku – prozrazením své aktuální polohy zjednodušení krádeže/zneužití vzdáleného majetku.

Psychický/poškození reputace

- prozrazení vlastních citlivých/intimních informací – intimní fotografie, video, záznam intimní komunikace;
- prozrazení cizích citlivých/intimních informací – intimní fotografie, video, záznam intimní komunikace.

Ztráta zaměstnání

- prozrazení tajných/interních firemních informací – prozrazení citlivých informací jako jsou rodná čísla klientů, obchodní tajemství;
- citlivých/intimních osobních informací – intimní fotografie, video, záznam intimní komunikace.

3.3.3 Motivace bezpečnosti provozovatelů sociálních sítí

Co nutí/motivuje provozovatele sociálních sítí, aby udržovaly sociální sítě bezpečné:

- Pozornost a zájem uživatelů;
- Legislativní požadavky státu a úřadů;
- Image a reputace sociální sítě;
- Sociální/veřejná odpovědnost, strategie společnosti.

Co odrazuje/demotivuje provozovatele sociálních sítí, aby udržovaly sociální sítě bezpečné:

- Náklady na zaměstnance a použité technologie;
- Možné problémy s kompatibilitou;
- Náklady na testování
- Změna chování aplikací;
- Možná ztráta uživatelů díky jinému (horšímu) ovládání.

3.4 Doporučená opatření

Tato kapitola obsahuje doporučená opatření pro uživatele sociálních sítí, které vyplývají se Seznamu hrozeb, Analýzy rizik. a Zhodnocení rizik.

3.4.1 Seznam opatření

Tabulka 8 Seznam opatření (Zdroj: Vlastní zpracování)

Seznam opatření pro bezpečnost sociálních sítí	
Název opatření	**Popis opatření**
Hodnocení citlivosti informací	Uživatel by měl zhodnotit informace, které je vhodné na sociálních sítích zveřejňovat s ohledem na možné riziko jejich veřejného prozrazení, zneužití, krátkodobé/dlouhodobé nedostupnosti či jejich úplné ztráty.
Vytvoření skupin	Uživatel by měl vytvořit skupiny uživatelů, se kterými chce

přátel	informace sdílet. Například na skupiny: Veřejnost, Rodina, Přátelé, Známí, Pracovní kolegové. A následně jasně definovat, jaké informace s určenými skupinami bude sdílet, viz opatření „Hodnocení bezpečnosti informací“. Při komunikaci s neznámi uživateli na sociálních sítích by měl uživatel prověřit reálnost uživatele a jeho přátel. Měl by brát i v potaz, že si lze virtuální přátele vytvořit nebo koupit.
Definování informací pro sdílení se skupinami uživatelů	Uživatel by měl informace, které vyhodnotil z pohledu jejich citlivosti jako přípustné pro sdílení na sociální síti dle opatření „Hodnocení informací“, dále rozdělit pro sdílení mezi skupinami uživatelů, které definoval v opatření *Vytvoření skupin přátel*. Například rodinné fotografie sdílet pouze se skupinou Rodina, pracovní dokumenty pouze se skupinou Pracovní kolegové, oblíbený článek zveřejněný na internetu se skupinou Veřejnost atp. Při komunikaci s neznámi uživateli na sociálních sítích by měl uživatel prověřovat reálnost uživatele, jeho přátel a brát v potaz, že si lze virtuální přátele vytvořit nebo koupit.
Kontrola práv sdílených informací	Uživatel by měl kontrolovat nastavení účtu na sociální síti, zejména nastavení sdílení obsahu s veřejností. V rámci kontroly by měl jako nepřihlášený a přihlášený cizí uživatel sociální sítě zkontrolovat rozsah svých informací, které jsou ostatním viditelné, aby si prakticky ověřil správnost pravidel pro sdílení informací na sociální síti.
Přístup k účtu pouze důvěryhodným aplikacím	Uživatel by měl povolit přístup k uživatelskému účtu pouze bezpečným aplikacím třetích stran. Jedná se například miniaplikace třetích stran pro systém Windows, či mobilní platformy Android, iOS a Mobile Phone. Týká se to též například her nabízených Facebooku.

Přístup pouze z bezpečných zařízení	Uživatel by měl povolit přístup k uživatelskému účtu sociální sítě pouze bezpečným zařízením. Za nebezpečné zařízení lze označit například sdílené PC na pracovišti či kavárně, cizí mobilní telefon/tablet. Taktéž by měl v nastavení sociální sítě kontrolovat nastavená pravidla a povolená zařízení. Při odcizení či ztrátě zařízení, by měl ze seznamu důvěryhodných zařízení sociální sítě zařízení neprodleně odebrat.
Šifrované spojení	Datové spojení mezi koncovou uživatelskou aplikací a provozovatelem sociální sítě by mělo být šifrováno (SSL, TLS) alespoň šifrováním 128 bit AES nebo jiným ekvivalentním šifrováním.
Návštěva pouze bezpečných odkazů	Uživatel by měl navštěvovat pouze bezpečné odkazy. Pokud uživateli pošle neznámý uživatel odkaz, dá se předpokládat, že právě tento odkaz může vést na nebezpečnou stránku, například obsahující malware. Nelze ale spoléhat ani na odkazy od důvěryhodných přátel. Odkaz na nebezpečnou stránku mohou důvěryhodné osoby odeslat buď z neznalosti nebezpečnosti stránky, nebo jejich účet již může být zneužit a odkaz odeslán útočníkem s cílem získání další oběti.
Nezveřejňování aktuální polohy uživatele	Uživatel by neměl na sociální síti zveřejňovat svoji aktuální polohu, pokud si není vědom možných dopadů (vykradení bytu atp.).
Vypnutí možnosti určování geolokační polohy ostatním uživatelům/aplikacím	Vypnutí možnosti zjišťování a zveřejňování polohy uživatele třetí stranou. Jedná se například o možnost lokalizovat uživatele bez jeho vědomí ať už uživateli sociální sítě nebo aplikacemi. Týká se to taktéž aplikací třetích stran (hry, aplikace).
Ověření totožnosti uživatele	Při navazování prvního kontaktu přes sociální síť s novým uživatelem se doporučuje ověřit jeho pravou identitu.

	Například přes telefonní hovor nebo na základě informací, které mohou znát jen dvě komunikující osoby (zážitky z dětství, interní pracovní specifikum atp.). Též lze nového uživatele ověřit pomocí doporučení od důvěryhodné osoby.
Silné heslo	Pro přihlášení k účtu sociální sítě se doporučuje požívat alespoň 10místné heslo, které obsahuje velká, malé písmena, číslice a alespoň jeden speciální znak. Heslo by se mělo alespoň čtvrtletně měnit a nemělo by se opakovat.
Vícefaktorová autentizace	K přihlášení k účtu sociální sítě by měl uživatel používat vícefaktorovou autentizaci (prostřednictvím SMS, generátoru hesla, atp.) pokud to nastavení autentizace umožňuje.
Aktualizované aplikace	Uživatel by měl udržovat operační systém a aplikace stále aktuální. Doporučuje se mít stále zapnuté automatické stahování a spouštění aktualizací.
Kontrola aplikačních oprávnění	Uživatel by měl před instalací aplikace zjistit přístupová oprávnění aplikace a až po zhodnocení rizik se rozhodnout, zdali si aplikaci nainstaluje. Na zvážení jsou zejména atributy jako přístup do kalendáře, kontaktů, určování polohy, posílání zpráv (SMS, email, instant messaging apod.), použití přihlašovacích údajů, vytváření uživatelských účtů, přístup do paměti zařízení aj. Oprávnění by měl uživatel kontrolovat i v rámci aktualizací, jelikož se oprávnění mohou s verzemi aplikace měnit.
Uzamčení obrazovky	Uživatel by měl na zařízení, kde používá aplikaci pro přístup do sociální sítě, používat automatické uzamykání obrazovky PINem či heslem. Obrazovka zařízení by se měla automaticky uzamknout po jedné minutě nečinnosti.
Vzdělávání v rámci bezpečnosti	Uživatel by měl sledovat dění ohledně bezpečnosti na sociálních sítích aby dokázal adekvátně reagovat na nové bezpečnostní hrozby. Například čtením zpravodajských webů

	jako jsou Lupa.cz, Zive.cz atp.
Hledání a zneplatnění podvržené uživatelské identity	Uživatel by měl kontrolovat, zdali se za jeho identitu nevydává někdo cizí. Pokud falešnou identitu najde, měl by požádat provozovatele sociální sítě o její smazání.
Zálohování informací	Uživatel by měl zálohovat informace, které jsou uložené na sociální síti. Jednak pro případ jejich úplné ztráty, nebo pro případ výpadku sociální sítě.
Záložní plán pro výpadek sociální sítě	Pro případ výpadku sociální sítě by mělo být definováno záložní řešení, jak funkci sociální sítě nahradit. Týká se zejména firem a jejich plánů Business Continuity.
Ověřování zpráv	Pravdivost a důvěryhodnost zpráv, které se šíří sociální sítí, by měl uživatel prověřovat, aby nenaletěl na podvodné nabídky, či na poplašené zprávy a taktéž aby je dál nešířil, případně na jejich nebezpečí upozornil ostatní.
Znalost pravidel a nastavení sociální sítě	Uživatel by měl znát pravidla a možnosti nastavení sociální sítě. Měl by též předpokládat, že provozovatel sociální sítě může průběžně pravidla a možnosti nastavení uživatelského účtu měnit.

3.4.2 Přiřazení opatření k identifikovaným rizikům

V této kapitole jsou k vypočteným rizikům z kapitoly Analýza rizik přiřazena doporučená opatření. V tabulce doporučených opatření níže jsou v levém sloupci uvedeny názvy hrozeb, v horním pravém řádku pak názvy opatření. Prostřednictvím znaménka x jsou vytvořeny vazby mezi riziky a opatřeními, kterými lze rizika buď zmírnit, nebo zcela eliminovat. Pokud se uživatel rozhodne rizika hodnocená v kapitole Analýza rizik řídit, měl by pro minimalizaci či úplnou eliminaci rizik použít opatření podle níže v tabulce uvedeného klíče.

Tabulka 9 Vazby doporučených opatření vůči hodnoceným rizikům první část (Zdroj: Vlastní zpracování)

	Doporučená opatření část 1.									
Název hrozby	**Hodnocení citlivosti informací**	**Vytvoření skupin přátel**	**Definování informací pro sdílení se skupinami uživatelů**	**Kontrola práv sdílených informací**	**Přístup k účtu pouze důvěryhodným aplikacím**	**Přístup pouze z bezpečných zařízení**	**Šifrované spojení**	**Návštěva pouze bezpečných odkazů**	**Nezveřejňování aktuální polohy uživatele**	**Vypnutí možnosti určování geolokační polohy ostatním uživatelům/aplikacím**
Falšování identity										
Sledování chování uživatele	x	x	x	x	x	x	x	x	x	x
Šíření nepravdivých informací, vyvolání paniky										
Šíření malwaru					x	x		x		
Sledování chování lidí	x	x	x	x	x	x	x	x	x	x
Únik citlivých informací prostřednictvím chyby třetí strany	x	x	x	x	x					
Narušení bezpečností strategie/bezpečnosti firmy	x	x	x	x	x	x	x	x		

Vědomé zveřejnění vlastních citlivých informací samotným uživatelem	x	x	x	x	x	x	x		x	x
Prozrazení aktuální polohy uživatele jeho přáteli	x		x						x	x
Prolomení/nedostatečné zabezpečení sociální sítě							x			
Ztráta/odcizení zařízení s přístupem na sociální sítě						x				
Odcizení identity					x	x	x	x		
Změna možností nastavení uživatelského účtu				x						
Únik citlivých informací prostřednictvím chyby uživatele				x						
Sdílení přístupových údajů				x						
Prozrazení aktuální polohy uživatele samotným uživatelem	x		x	x						

Tabulka 10 Vazby doporučených opatření vůči hodnoceným rizikům druhá část (Zdroj: Vlastní zpracování)

		Doporučená opatření část 2.									
Název hrozby	**Silné heslo**	**Vícefaktorová autentizace**	**Aktualizované aplikace**	**Kontrola aplikačních oprávnění**	**Uzamčení obrazovky**	**Antimalwarová ochrana**	**Vzdělávání v rámci bezpečnosti**	**Hledání a zneplatnění podvržené uživatelské identity**	**Zálohování informací**	**Záložní plán pro výpadek sociální sítě**	**Ověřování zpráv**
Falšování identity								x			
Sledování chování uživatele	x	x	x	x	x	x	x				
Šíření nepravdivých informací, vyvolání paniky							x				x
Šíření malwaru			x			x	x				
Sledování chování lidí	x	x	x	x	x	x	x	x			x
Únik citlivých informací prostřednictvím chyby třetí strany											
Narušení bezpečností strategie/bezpečnosti firmy	x	x			x	x	x	x	x	x	

Vědomé zveřejnění vlastních citlivých informací samotným uživatelem				x	x	x	x				
Prozrazení aktuální polohy uživatele jeho přáteli											
Prolomení/nedostatečné zabezpečení sociální sítě	x	x									
Ztráta/odcizení zařízení s přístupem na sociální sítě	x	x			x				x		
Odcizení identity	x	x	x	x	x	x	x				
Změna možností nastavení uživatelského účtu				x							
Únik citlivých informací prostřednictvím chyby uživatele							x				
Sdílení přístupových údajů	x	x					x				
Prozrazení aktuální polohy uživatele samotným uživatelem											

3.4.3 Obecná doporučení pro zaměstnance společnosti

Tato kapitola obsahuje obecná doporučení pro uživatele sociálních sítí.

- Pokud chcete, aby informace (například citlivé nebo tajné informace) byly v bezpečí, neumisťujte tyto informace na sociální sítě.
- Přesvědčte se, jaké informace sdílíte veřejně a to tím, že se podíváte na svůj účet bez přihlášení (jako cizí osoba). Tedy tak, jak jej vidí ostatní uživatelé.
- Jasně si definujte uživatele, se kterými chcete sdílet neveřejné informace.
- Přístup k účtu sociální sítě povolte pouze důvěryhodným aplikacím a zařízením (PC, notebook, tablet, mobilní tel. apod.)
- K sociálním sítím přistupujte prostřednictvím zabezpečeného připojení HTTPS.
- Navštěvujte pouze odkazy zaslané od důvěryhodných uživatelů.
- Ani zprávy zasílané od důvěryhodných přátel nemusí být bezpečné. Nikdy nevíte, zdali jejich účet nebyl kompromitován, a zdali vám útočník nezaslal nebezpečný odkaz prostřednictvím důvěryhodné identity. Taktéž předpokládejte, že legitimní uživatel vám může zaslat nebezpečnou zprávu v dobré víře, bez vědomí jeho hrozícího nebezpečí.
- Zakažte sociálním sítím, případně aplikacím třetích stran mobilních zařízení lokalizovat a zveřejňovat vaši aktuální polohu.
- Nezveřejňujte konkrétní informace typu plánování osobního času, citlivé osobní informace týkající se například resetování hesla (jméno psa, rodné jméno matky…) atp.
- Při komunikaci přes sociální sítě si ověřte, zdali komunikujete opravdu s osobou, za kterou se avatar (digitální identita) vydává.
- Pro přihlášení používejte silná hesla, popřípadě více faktorovou autentizaci.
- Používejte aktualizovaný operační systém, webový prohlížeč a antivirový program.
- Měňte často (alespoň čtvrtletně) přístupové heslo

1.1.1.1 Opatření prostřednictvím infografiky

Bezpečnostní doporučení nemusejí být prezentována pouze textovou formou ale i grafickou. Jeden z příkladů, kdy je pro prezentaci protiopatření použita infografiky, je uveden níže. Tato forma sdělení může být daleko efektivnější než strohé textové sdělení.

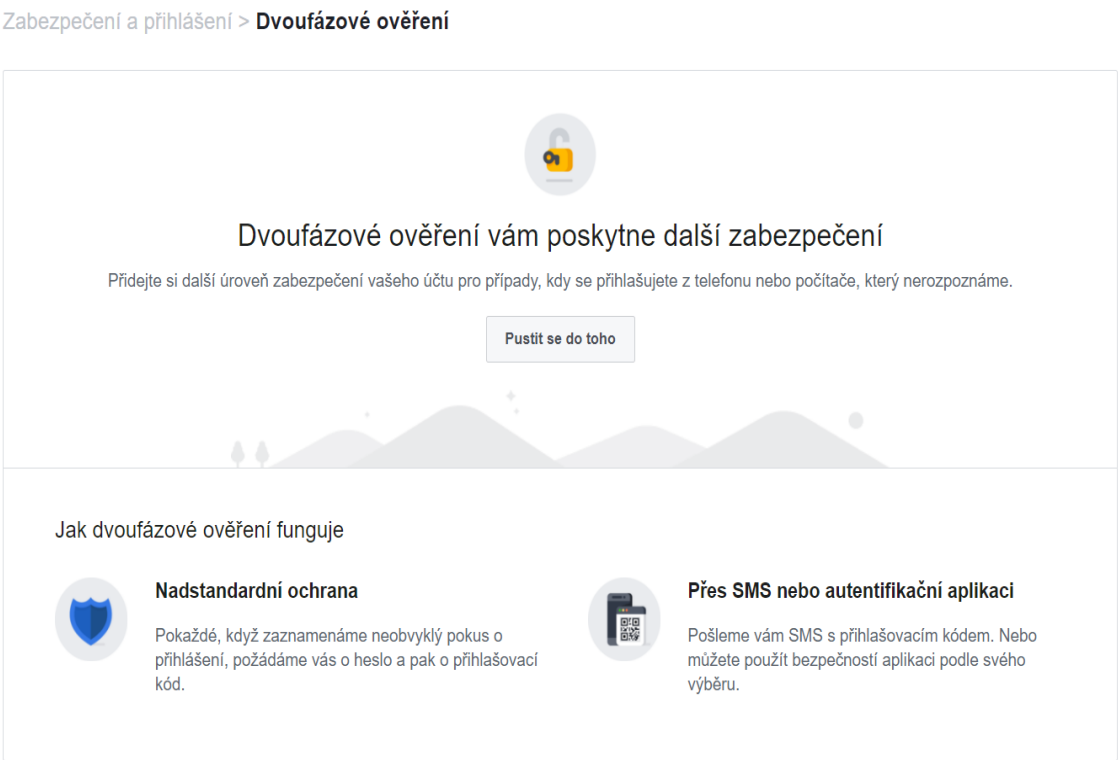
Obrázek 10 Příklad opatření pro uživatele sociálních sítí prostřednictvím infografiky. (Zdroj: www.techrepublic.com)

3.4.4 Konkrétní doporučení pro bezpečné užívání sociální sítě Facebook

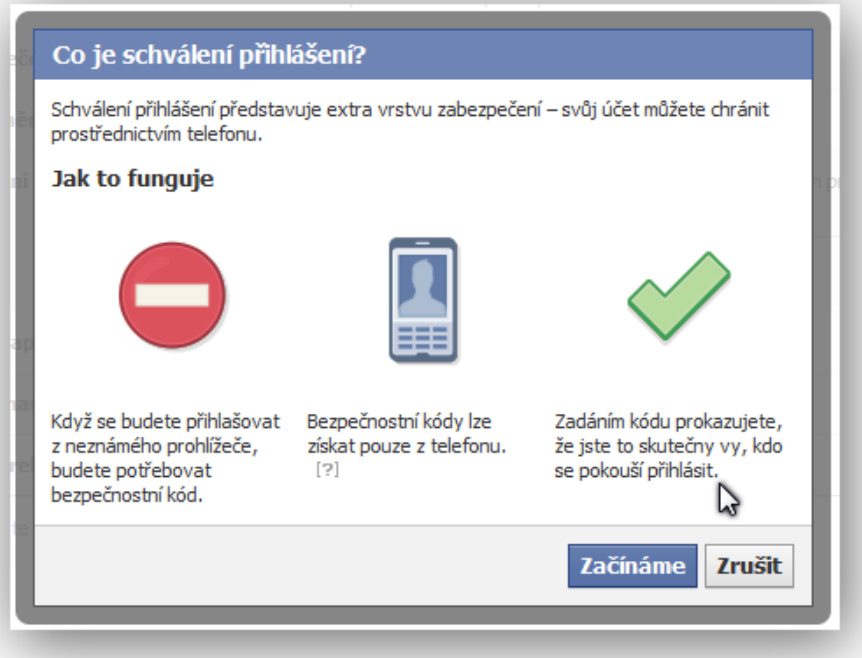
Všichni zaměstnanci popsané firmy uvedli, že používají síť Facebook, ale málokdo z nich věděl o všech možnostech, jak zabezpečit svůj profil na této síti. Z tohoto důvodu jsem si říkal, že by bylo vhodné udělat seznam možností, jak zabezpečit osobní profily na Facebook. Níže jsou uvedena konkrétní doporučení pro zaměstnance společnosti při používání sociální sítě Facebook.

1.1.1.2 Vícefaktorová autentizace s pomocí mobilního telefonu

Pro větší bezpečnost přihlašování do sociální sítě zapněte funkci vícefaktorové autentizace, například přihlášení prostřednictvím SMS nebo důvěryhodnou aplikací, zpravidla poskytovanou provozovatelem sociální sítě. Například na Facebooku zapnete vyžadování bezpečnostní kódu pro přístup k účtu na kartě *Zabezpečení*, aktivací volby *dvoufázové přihlášení*. Při aktivaci funkce budete provedeni průvodcem aktivací generátoru kódů a otestováním funkčnosti autentizace, viz obrázky níže.

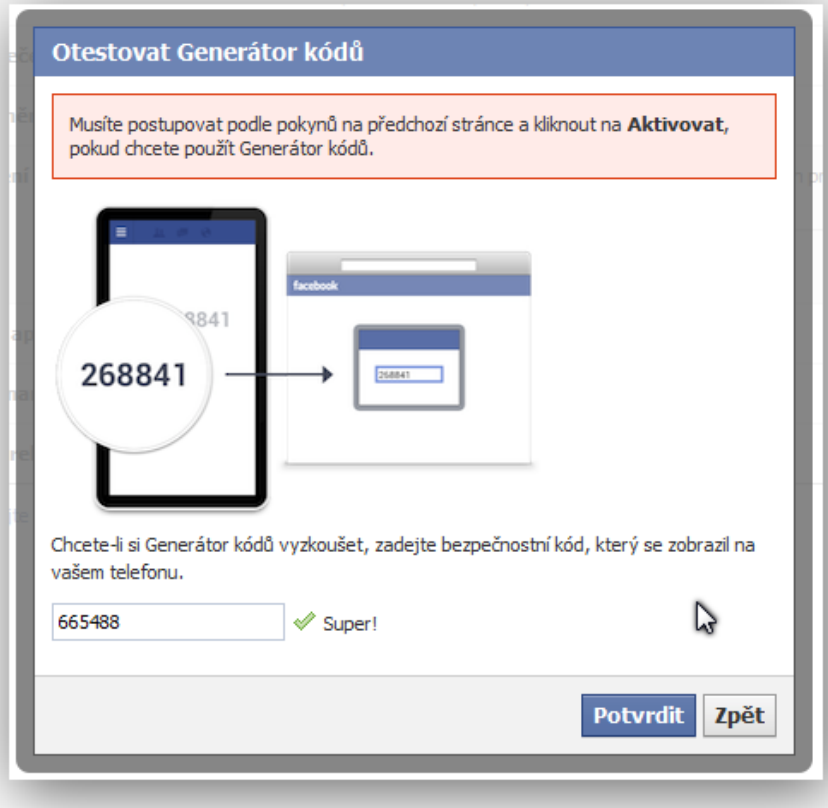


Obrázek 11 Nastavení dvoufázového zabezpečení při přihlašování do sociální sítě Facebook. (Zdroj: www.facebook.com)



Obrázek 12 Popis autentizace zadáváním kódu při přihlašování do sociální sítě Facebook. (Zdroj: www.facebook.com)

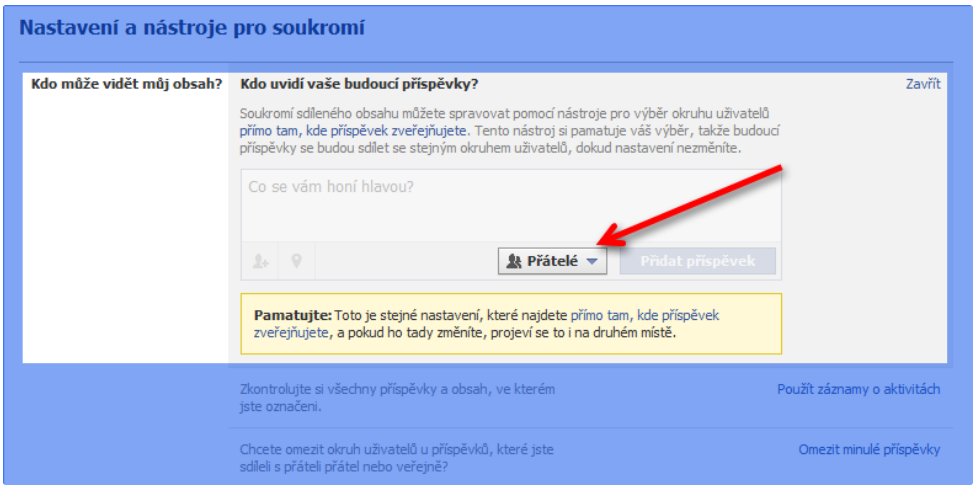
Obrázek 13 Aktivace generátoru kódů pro přihlašování do sociální sítě Facebook. (Zdroj: www.facebook.com)



Obrázek 14 Vložení kódu z mobilní aplikace do přihlašovacího dialogu sociální sítě Facebook. (Zdroj: www.facebook.com)

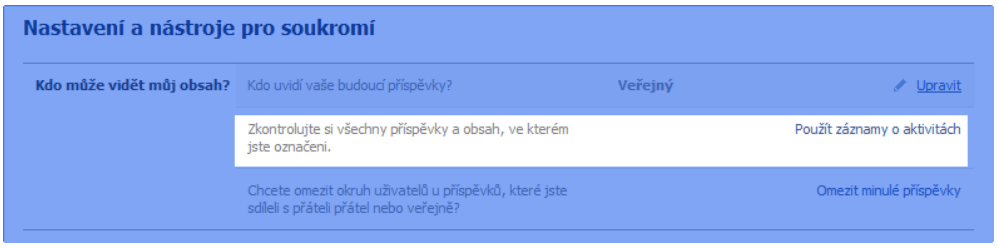
3.4.4.1 Kontrola viditelnosti obsahu

Pro budoucí příspěvky, které budete na Facebook vkládat, lze přednastavit jejich viditelnost (*Nastavení soukromí -> Soukromí -> Kdo může vidět můj obsah? -> Kdo uvidí vaše budoucí příspěvky?*). Pokud nechcete, aby vaše příspěvky nebyly primárně zobrazovány jako Veřejné (příspěvky budou přístupné veřejnosti), můžete jejich viditelnost zúžit například pouze vybrané uživatelské skupiny, například na *Přátele* či jinou vámi definovanou uživatelskou skupinu. V nejstriktnějším případě lze nastavit viditelnost pouze na vaši osobu, tedy viditelnost *Pouze já*.



Obrázek 15 Nastavení viditelnosti budoucích vložených příspěvků.
(Zdroj: www.facebook.com)

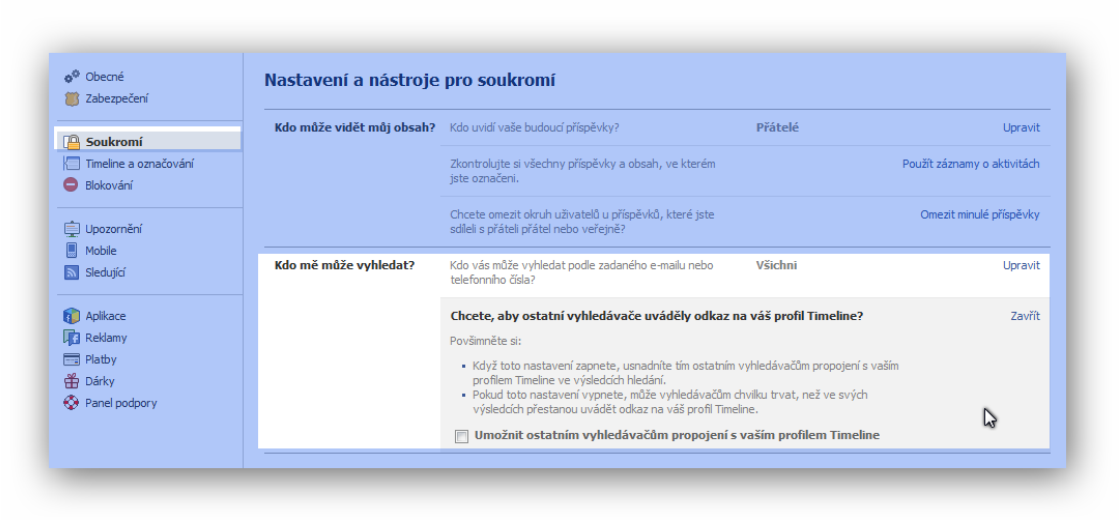
Pokud byste chtěli zkontrolovat, či změnit viditelnost již vložených příspěvků, lze jejich editaci provést prostřednictvím volby *Zkontrolujte si všechny příspěvky a obsah, ve kterém jste označeni*. (*Nastavení soukromí -> Soukromí -> Kdo může vidět můj obsah?*). Můžete tak změnit zpětně viditelnost příspěvků, které jste vložili v minulosti, nebo příspěvky zcela vymazat.



Obrázek 16 Možnost editace viditelnosti příspěvků vložených v minulosti.
(Zdroj: www.facebook.com)

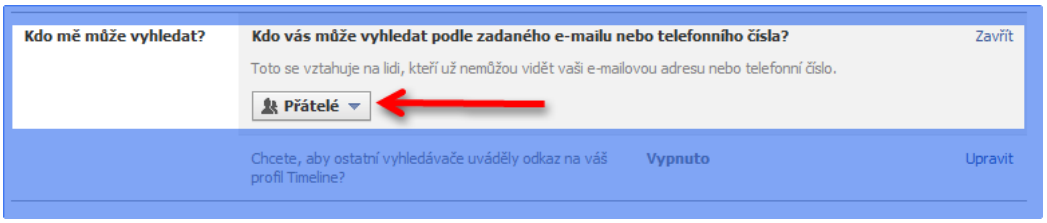
3.4.4.2 Zákaz vyhledávání

Pokud chcete, aby identita na sociální síti nebyla dohledatelná mimo sociální síť, například přes vyhledávače Google či Seznam, zakažte možnost její veřejné vyhledání přes volbu *Soukromí -> Kdo mě může vyhledat? -> Chcete, aby ostatní vyhledávače uváděly odkaz na váš profil Timeline?* Nutno podotknout, že konkrétně tato volba na Facebooku pouze znemožní vyhledání samotné identity. Veškerá data, která jsou danou identitou na sociální síti veřejná, dále veřejná zůstanou, tudíž budou volně přístupná všem uživatelům kyberprostoru.



Obrázek 17 Zákaz vyhledávání (Zdroj: www.facebook.com)

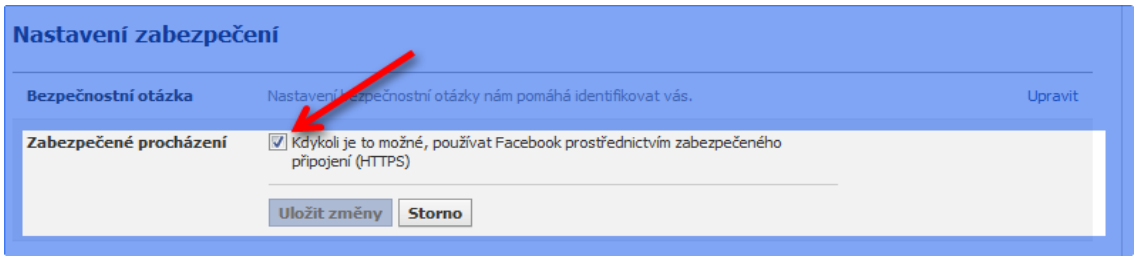
Pokud si nepřejete, aby vás mohli vyhledat podle e-mailu nebo telefonního čísla, které jste zadali do svého pofilu na Facebooku, pouze *Přátelé*, nikoli už *Přátelé přátel* nebo dokonce všichni uživatelé Facebooku, vyberte u položky *Kdo vás může vyhledat podle zadaného e-mailu nebo telefonního čísla?* (*Nastavení soukromí -> Kdo mě může vyhledat?*) volbu *Přátelé*.



Obrázek 18 Určení skupiny uživatelů Facebooku, kteří váš uživatelský profil budou moci vyhledat (Zdroj: www.facebook.com)

3.4.4.3 Zabezpečené spojení

Pro bezpečné datové spojení mezi servery poskytovatele sociální sítě Facebook a uživatelskou koncovou aplikací (webový prohlížeč, miniaplikace Windows, mobilní aplikace pro Android, iOS atp.) zapněte požadavek na šifrované spojení https. Aktivaci šifrování provede zatržením volby *Nastavení zabezpečení -> Zabezpečené procházení*.

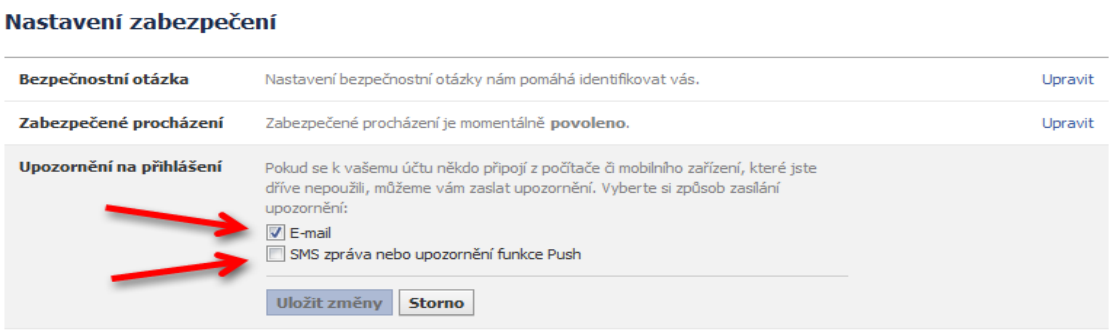


Obrázek 19 Aktivace zabezpečeného spojení v rámci protokolu https

(Zdroj: www.facebook.com)

3.4.4.4 Upozornění na přihlášení

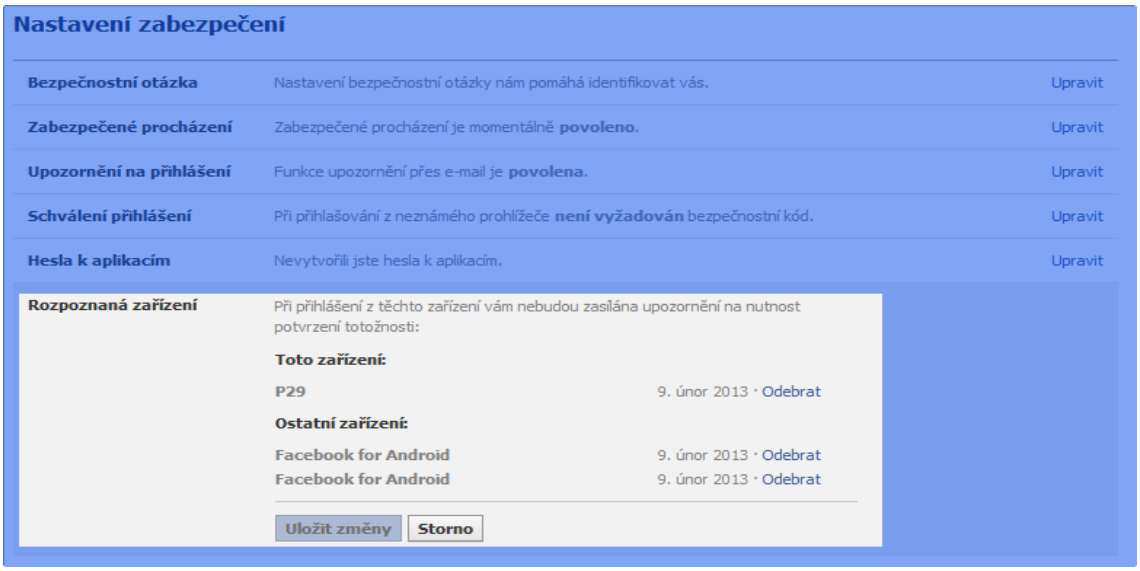
Pro případ, že by se vašich autentizačních údajů zmocnila cizí osoba a přihlásila se k vašemu uživatelskému profilu, je dobré mít aktivovanou funkci *Upozornění na přihlášení* (*Nastavení zabezpečení*). V rámci funkce je majitel uživatelského profilu vždy informován, buď prostřednictvím e-mailu nebo SMS, o připojení k uživatelskému účtu ze zařízení, které se do té doby k uživatelskému profilu nepřipojilo. Uživatel je tak při možné kompromitaci uživatelského profilu ihned informován. Může tak okamžitě reagovat na nastalou situaci například změnou autentizačních údajů.



Obrázek 20 Nastavení zasílání upozornění při přístupu k uživatelskému účtu z neznámého zařízení.

(Zdroj: www.facebook.com)

Lze též spravovat již rozpoznaná zařízení, a to v nabídce *Rozpoznaná zařízení (Nastavení zabezpečení).* Je vhodné seznam rozpoznaných zařízení průběžně kontrolovat. Kontrolou může být odhaleno nežádoucí zařízení, prostřednictvím kterého může například probíhat kompromitace uživatelského profilu.



Obrázek 21 Seznam rozpoznaných zařízení, kterým je povolen přístup k uživatelskému profilu. (Zdroj: www.facebook.com)

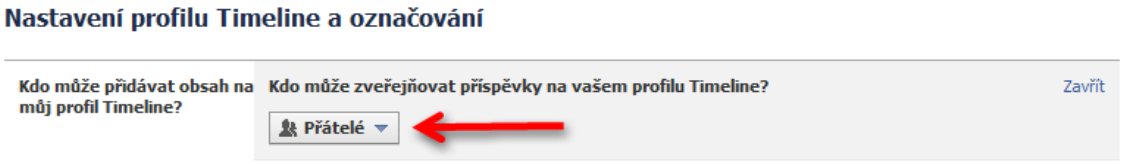
3.4.4.5 Kontrola aktivních relací

Uživatel by měl pravidelně kontrolovat relace (čas, místo a typ zařízení) v rámci kterých je přistupováno k uživatelskému profilu (*Nastavení zabezpečení -> Aktivní relace*). Pravidelnou kontrolou lze předejít či včasně zakročit proti případné kompromitaci uživatelského profilu. Nežádoucí relace je možné v případě potřeby neodkladně ukončit kliknutím na volbu *Ukončit aktivitu* viz obrázek.

Obrázek 22 Kontrola aktivních relací (Zdroj: www.facebook.com)

3.4.4.6 Definování práv pro Timeline

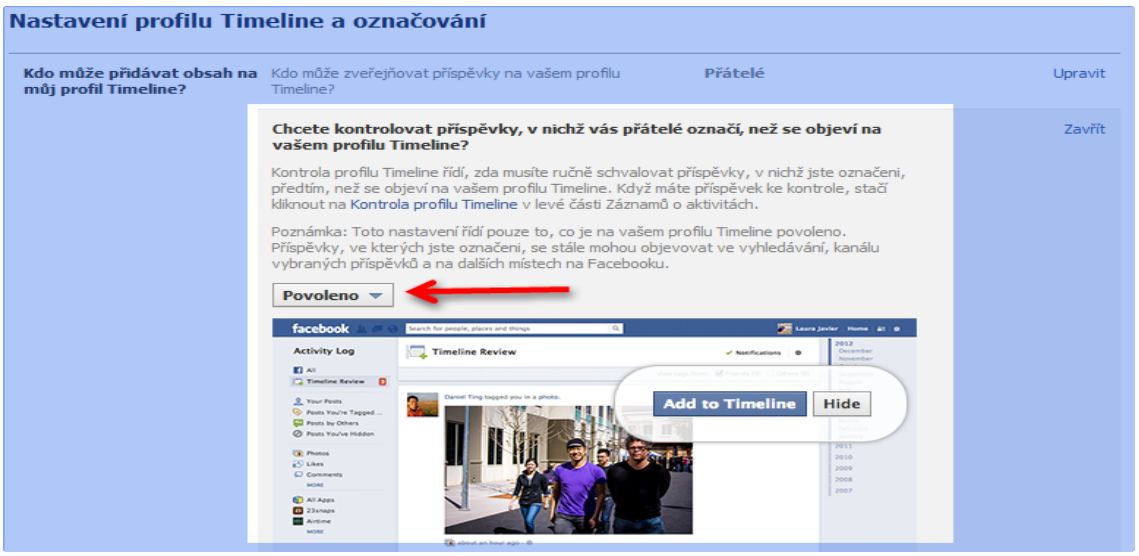
Definujte skupinu důvěryhodných uživatelů (*Timeline označování -> Kdo může přidávat obsah na můj profil Timeline?*), kterým dovolíte vkládat příspěvky na vaši Timeline. Předejdete tak tomu, že vám někdo cizí na Timeline vloží příspěvek s nevhodnou tématikou či dokonce s nebezpečným obsahem. Nevhodný/nebezpečný obsah by mohl poškodit vaši pověst před ostatními uživateli či veřejností. V horším případě by mohl vést až k zablokování vašeho uživatelského profilu z důvodu šíření nebezpečného/nelegálního obsahu.



Obrázek 23 Nastavení oprávnění pro vkládání příspěvků na Timeline (Zdroj: www.facebook.com)

3.4.4.7 Aktivace kontroly příspěvků, kde jste označeni

Aktivujte si kontrolu příspěvků (*Timeline označování -> Kdo může přidávat obsah na můj profil Timeline?*), v rámci které musíte ručně schvalovat příspěvky, v nichž jste označeni, předtím, než se objeví na vašem profilu Timeline. Předejte tak zveřejňováním příspěvků, které byste rádi viděli pouze jako privátní.

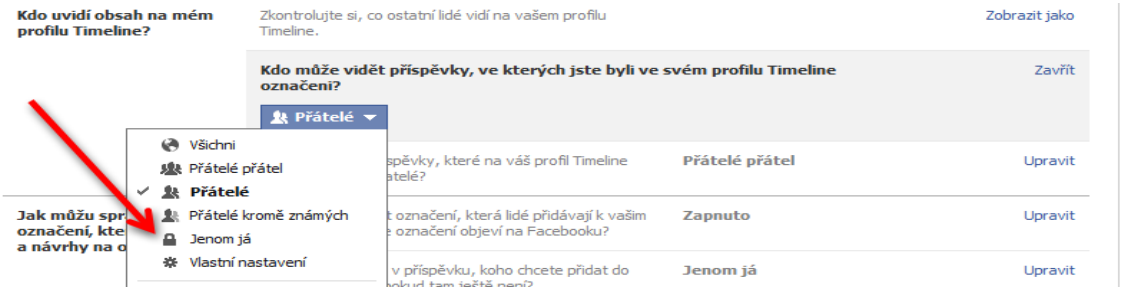


Obrázek 24 Nastavení ručního schvalování příspěvků na nichž jste označeni. (Zdroj: www.facebook.com)

Berte ale na vědomí, že toto nastavení se týká pouze vašeho profilu Timeline. Příspěvky, ve kterých jste označeni, se stále mohou objevovat ve vyhledávání, kanálu vybraných příspěvků a na dalších místech na Facebooku.

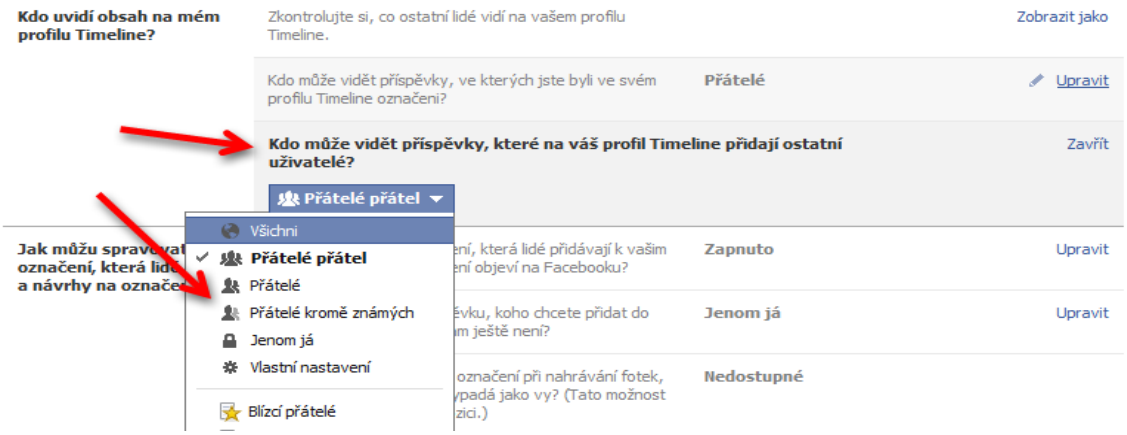
3.4.4.8 Viditelnost příspěvků na Timeline

Pro příspěvky, na kterých jste označeni, nastavte viditelnost (*Timeline označování -> Kdo uvidí obsah na mém profilu Timeline? -> Kdo může vidět příspěvky, ve kterých jste byli ve svém profilu Timeline označeni?*) pouze pro ty osoby/skupiny, kterým můžete důvěřovat, že daný příspěvek nezneužijí. Popřípadě zvolte nastavení *Jenom já*, příspěvky, v rámci kterých jste označeni na Timeline pak uvidíte jenom vy.



Obrázek 25 Nastavení viditelnosti příspěvků, na kterých jste označeni. (Zdroj: www.facebook.com)

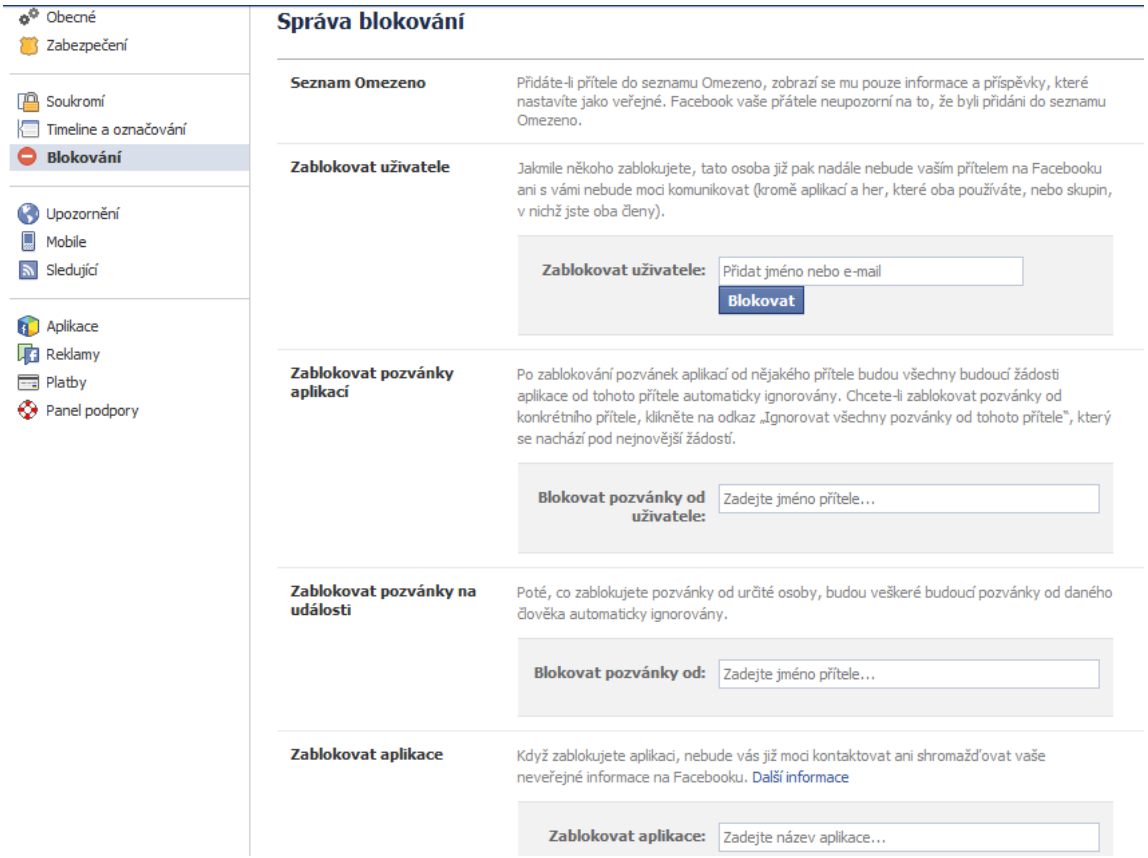
Pro viditelnost příspěvků, které na váš profil Timeline přidají ostatní uživatelé, nastavte též oprávnění dle návodu výše (*Timeline označování -> Kdo uvidí obsah na mém profilu Timeline? -> Kdo může vidět příspěvky, které na váš profil Timeline přidají ostatní uživatelé?*).



Obrázek 26 Nastavení viditelnosti příspěvků, které na vaši Timeline vložili ostatní uživatelé. (Zdroj: www.facebook.com)

3.4.4.9 Blokování uživatelů, aplikací, pozvánek

V případě, že váš obtěžuje některý uživatel sociální sítě, jeho pozvánky na aplikace a události, či samotné aplikace, můžete jej zablokovat v rámci *Správy blokování* viz obrázek. Zamezíte tím komunikaci s uživatelem samotným (funkce *Zablokovat uživatele)*, zablokujete zasílání pozvánek do aplikací od uživatele (funkce *Zablokovat pozvánky aplikací)*, zablokujete zasílání pozvánek na události od uživatele (funkce *Zablokovat pozvánky na události*), či zablokujete aplikaci (funkce *Zablokovat aplikace*), která již vás nebude moci kontaktovat ani shromažďovat vaše neveřejné informace na Facebooku.



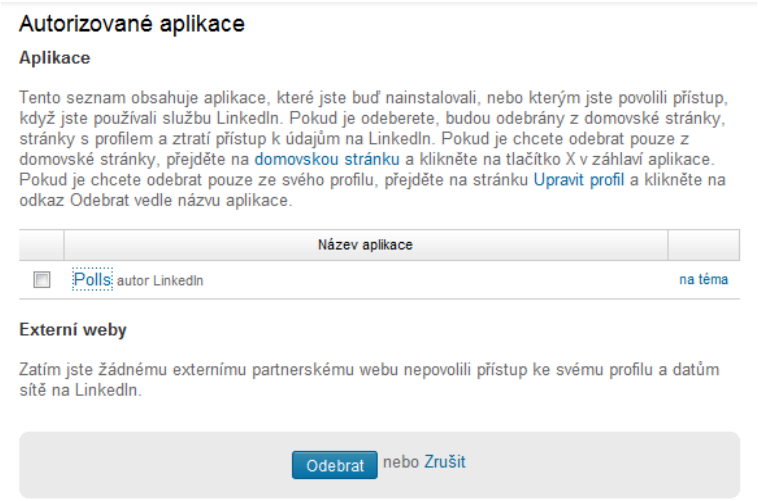
Obrázek 27 Správa blokování uživatelů sociální sítě, pozvánek a aplikací. (Zdroj: www.facebook.com)

3.4.5 Konkrétní doporučení pro sociální síť LinkedIn

Níže jsou uvedena konkrétní doporučení pro uživatele sociální LinkedIn.

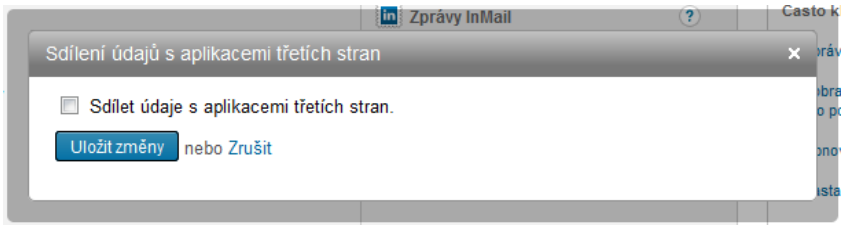
3.4.5.1 Kontrola autorizovaných aplikací

Pravidelně kontrolujte na záložce *Autorizované aplikace* (*Nastavení->Skupiny, společnosti, aplikace->Aplikace->Zobrazit Vaše aplikace)* aplikace, které mají přístup k vašemu účtu na sociální síti LinkedIn. Pokud v seznamu naleznete aplikace, které neznáte anebo je považujete za nedůvěryhodné, odeberte je. Zamezíte tak nežádoucím aplikacím přístup k vašim informacím na LinkedIn a tím i šíření informací mimo LinkedIn.



Obrázek 28 Seznam autorizovaných aplikací, které mají povolený přístup k informacím uživatelského účtu na sociální síti LinkedIn.
(Zdroj: www.linkedin.com)

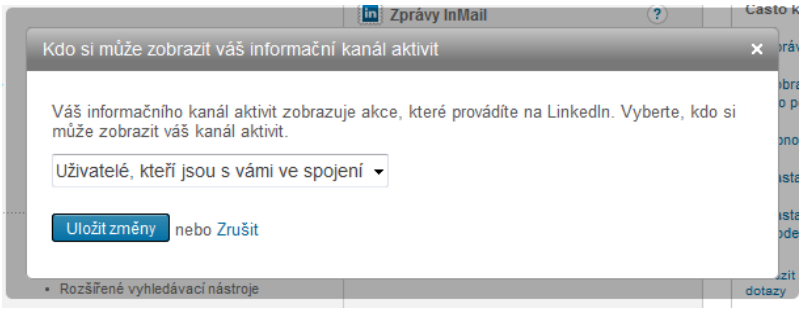
Pokud chcete přístup k informacím na sociální síti LinkedIn zakázat všem aplikacím třetích stran, můžete tak učinit na záložce *Sdílení údajů s aplikacemi třetích stran* (*Nastavení->Skupiny, společnosti a aplikace->Nastavení ochrany osobních údajů-> Zapnout/vypnout sdílení údajů s aplikacemi třetích stran*).



Obrázek 29 Zapnutí/vypnutí sílení údajů s aplikacemi třetích stran. (Zdroj: www.linkedin.com)

3.4.5.2 Nastavení odběru kanálu aktivit

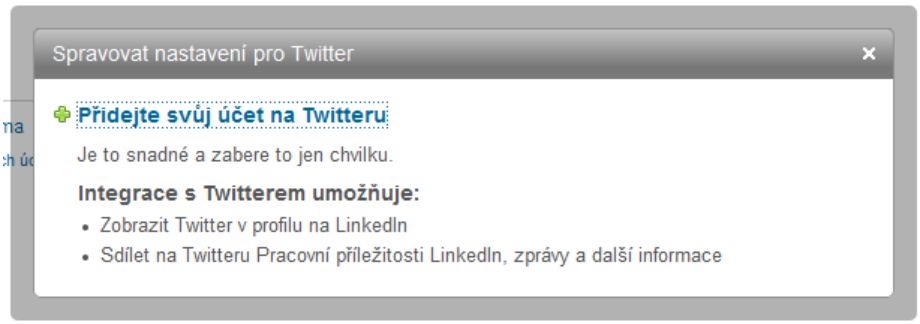
Na kartě *Vybrat, komu se zobrazuje informační kanál o vašich aktivitách* (*Nastavení->Profil-> Nastavení ochrany osobních údajů*) definujete skupinu uživatelů, kterým bude dovoleno zobrazovat akce, které vykonáváte na LinkedIn. Jedná se například o seznam přátel, informace o vašem uživatelském profilu a další informace které píšete na sociální sít LinkedIn. Určíte tím skupinu uživatelů sociální sítě LinkedIn, která bude mít přístup k vašemu kanálu aktivit. Ostatním uživatelům mimo definovanou skupinu nebudou informace zobrazovány.



Obrázek 30 Nastavení skupiny uživatelů, která bude moci odebírat informace o aktivitách daného uživatele. (Zdroj: www.linkedin.com)

3.4.5.3 Sdílení informací s Twitterem

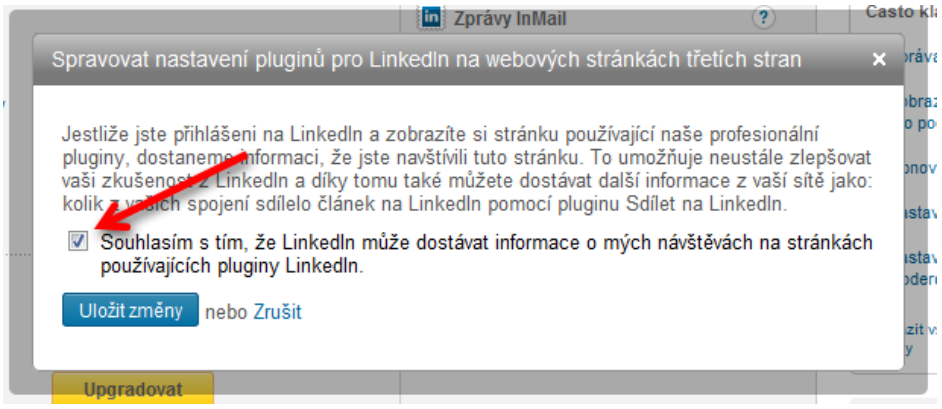
LinkedIn umožňuje sdílet informace (*Nastavení->Profil->Nastavení->Nastavení pro Twitter*) se sociální sítí Twitter. Pokud se rozhodne uvedené sociální sítě propojit, je před zrealizováním toho propojení potřeba vzít na vědomí rizika, která důsledku propojení vzniknou. Jedná se zejména o riziko prozrazení citlivých informací cizím osobám.



Obrázek 31 Nastavení sdílení informací se sociální sítí Twitter.
(Zdroj: www.linkedin.com)

3.4.5.4 Správa pluginů LinkedIn

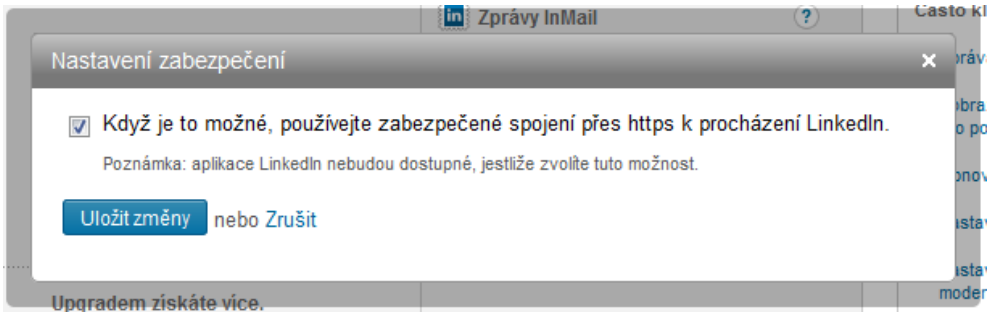
Sociální sít LinkedIn automaticky po vytvoření uživatelského účtu zapíná automatické mapování stránek, které uživatel navštíví. Sledování navštívených stránek probíhá prostřednictvím pluginů, které navštívené stránky obsahují. Pokud uživatel nechce, aby sociální síť LinkedIn mapovala navštívené webové stránky mimo síť LinkedIn, měl by deaktivovat tuto funkci v okně *Spravovat nastavení pluginů pro LinkedIn na webových stránkách třetích stran* (*Nastavení->Skupiny, společnosti a aplikace-> Nastavení ochrany osobních údajů-> Spravovat nastavení pluginů pro LinkedIn na webových stránkách třetích stran*) a to odškrtnutím zatržítka viz obrázek níže.



Obrázek 32 Odtržením zatržítka zakážete sociální síti LinkedIn sledovat vámi navštívené stránky.
(Zdroj: www.linkedin.com)

3.4.5.5 Zabezpečené spojení

Pro bezpečné datové spojení mezi servery poskytovatele sociální sítě LinkedIn a uživatelskou koncovou aplikací (webový prohlížeč, miniaplikace Windows, mobilní aplikace pro Android, iOS atp.) zapněte požadavek na šifrované spojení https. Aktivaci šifrování provede zatržením volby v okně *Nastavení zabezpečení (Nastavení->Účet->Nastavení-> Správa nastavení zabezpečení)* viz obrázek níže.



Obrázek 33 Aktivaci šifrovaného spojení při používání sociální stí LinkedIn ztržením zatržítka. (Zdroj: www.linkedin.com)

3.4.6 Ekonomické zhodnocení

Ekonomické zhodnocení zavedených proaktivních opatření, která slouží zejména ke zvyšování bezpečnostního povědomí uživatelů sociálních sítí, lze těžce přesně vyčíslit. Je to podobná situace jako při vyčíslování důsledků školení. Pokud jsou zaměstnanci správně proškoleni a úspěšně odolávají méně či více sofistikovaným kybernetickým útokům vedeným proti organizaci, je velice těžké takovou částku vůbec odhadnout. Tato práce se nezabývá návrhem ani implementací softwarového nebo hardwarového zabezpečení, ale slouží pouze jako podpora a návod pro zvyšování bezpečnostního povědomí při pohybu na sociálních sítích. Předpokládá se, že každý zaměstnanec, který přichází do styku se sociálními sítěmi, si prostuduje tuto práci a následkem toho se bude chovat mnohem obezřetněji.

Zavedení všech organizačních opatření v návrhové části jsou tedy bez dalších nákladů. Jediná činnost, na kterou bude nutné vyhradit finanční prostředky, je přítomnost lektora, který bude zaměstnance organizace školit za účelem zvyšování bezpečnostního povědomí.

ZÁVĚR

Cílem diplomové práce bylo zanalyzovat a zhodnotit bezpečnostní rizika sociálních sítí, zejména Facebook, LinkedIN a uvést bezpečnostní doporučení pro jejich uživatele.

V první kapitole CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ byla popsána metodika, podle které byla tato diplomová práce napsána.

V kapitole Sociální sítě byl vypracován popis, charakteristika a trendy sociálních sítí, konkrétněji pak popsány sociální sítě Facebook, Twitter a další sítě, které patří ohledně počtu uživatelů mezi nevětší sociální sítě.

V kapitole Rizika a hrozby sociálních sítí byly vyjmenovány známé incidenty a události, které se týkaly sociálních sítí. Na základě zmíněných incidentů a událostí byl pak v kapitole 2.7.2 sestaven seznam hrozeb, který byl dále využit v následující v analýze rizik. Seznam hrozeb byl čerpán z veřejně dostupných zdrojů, které o incidentech spojených se sociálními sítěmi informují, dále z praktických zkušeností uživatelů popisovaného podniku.

V kapitole Analýza rizik byla provedena analýza rizik sociálních sítí, která vycházela ze seznamu hrozeb sociálních sítí a z určené velikosti dopadu hrozeb, pravděpodobnosti jejich výskytu a pravděpodobnosti jejich úspěšnosti. Uvedené tři parametry byly stanoveny na základě pravděpodobných scénářů a jejich následného převedení na kvantitativní hodnoty pětistupňové škály prostřednictvím vodítek z tabulek: Tabulka 2 Stanovení číselné škály pravděpodobnosti výskytu hrozeb, Tabulka 3 Stanovení velikosti dopadu hrozeb, Tabulka 4 Stanovení číselné škály pravděpodobnosti úspěšnosti hrozeb Po stanovení parametrů velikosti dopadu, pravděpodobnosti výskytu a pravděpodobnosti úspěšnosti hrozeb, byly číselné hodnoty těchto tří parametrů vynásobeny, čímž byla stanovena hodnota velikosti rizika. Po výpočtu byla rizika dle jejich vypočtené velikosti sestupně seřazena a pro větší přehlednost dále rozčleněna.

V kapitole Zhodnocení

Zhodnocení rizik bylo provedeno zhodnocení vypočtených rizik z předešlé kapitoly. Podle pětistupňové škály velikosti rizik, byla tři nejvyšší rizika vyhodnocena jako vysoká rizika a jedno vyhodnoceno jako střední riziko. Zbylá rizika byla vyhodnocena jako Malá či Velmi malá.

Podrobnější informace o zhodnocení rizik jsou uvedeny v kapitole Zhodnocení výsledků analýzy rizik.

V kapitole Doporučená opatření byl sestaven Seznam opatření pro bezpečnost sociálních sítí, který obsahuje opatření pro minimalizaci či úplné potlačení výše hodnocených rizik. V tabulce Tabulka 9 Vazby doporučených opatření vůči hodnoceným rizikům pak byla na hodnocená rizika namapována relevantní opatření. Tím byla stanovena konkrétní opatření, díky kterých lze minimalizovat či zcela potlačit konkrétní rizika. V rámci praktické realizace řízení rizik sociálních sítí lze Tabulka 9 Vazby doporučených opatření vůči hodnoceným rizikům použít jako východisko.

V kapitole Obecná doporučení byl vytvořen seznam obecných doporučení pro uživatele sociálních sítí, který má sloužit jako základní uživatelský manuál pro bezpečné chování na sociální síti. V kapitole 3.4.4 a 3.4.5 pak byla stanovena konkrétní doporučení pro zaměstnance popsané společnosti, kteří používají sociální sítě LinkedIn a Facebook. Záměrem zmíněných dvou kapitol je poskytnout uživatelům uvedených dvou sociálních sítí doporučení pro důležitá bezpečnostní nastavení.

SEZNAM POUŽITÉ LITERATURY

(1) KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

(2) MARTÍNKOVÁ, Libuše a Václav PÍSECKÝ. *Kyberprostor jako náboženský prostor: průvodce chováním ve světě online*. Brno: L. Marek, 2007. Pontes pragenses (L. Marek). ISBN 978-80-87127-06-3.

(3) 3. ČASTORÁL, Zdeněk. *Management rizik v současných podmínkách*. Vydání I. Praha: Univerzita Jana Amose Komenského, 2017. ISBN 978-80-7452-132-4.

(4) 4. HAVLOVÁ, Jaroslava. sociální síť. *In: KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. Praha: Národní knihovna ČR, 2003 [cit. 2018-05-08]. Dostupné z: http://aleph.nkp.cz/F/?func=direct&doc_number=000015947&local_base=KTD

(5) Company Info. *Facebook Newsroom* [online]. 2018 [cit. 2018-04-16]. Dostupné z: http://newsroom.fb.com/company-info/

(6) BELLIS, Mary. Who Invented Facebook? The history behind the number one social media network Facebook. *About.com: Do more.* [online]. [cit. 2018-04-17]. Dostupné z: http://inventors.about.com/od/fstartinventions/a/Facebook.htm

(7) The Social Network. ČSFD.cz: *Česko-Slovenská filmová databáze* [online]. [cit. 2018-04-17]. Dostupné z: http://www.csfd.cz/film/262711-the-socialnetwork/

(8) 10 let s Facebookem. První kulaté narozeniny oslavil s miliardou lidí. Facebook magazín | *FaceMag.cz* [online]. [cit. 2018-04-17]. Dostupné z: http://facemag.cz/facebook-slavi-desate-vyroci-podivejte-se-na-jeho-historii/

(9) Exploring the software behind Facebook, the worlds largest site | Pingdom Royal. Pingdom Royal | We Love The Internet [online]. [cit. 2018-04-17]. Dostupné z: http://royal.pingdom.com/2010/06/18/the-software-behindfacebook/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed: +RoyalPingdom+(Royal+Pingdom)

(10) ZHAO, Haiping. HipHop for PHP: Move Fast - Facebook pro vývojáře. Vývojáři společnosti Facebook - *Facebook pro vývojáře* [online]. [cit. 2018-04-17]. Dostupné z: https://developers.facebook.com/blog/post/2010/02/02/hiphop-for-php--move-fast/73 12. JIANG, Changhao. BigPipe: Pipelining web pages for

high performance. Facebook [online]. [cit. 2018-04-17]. Dostupné z: https://www.facebook.com/notes/facebook-engineering/bigpipe-pipeliningweb-pages-for-high-performance/389414033919/

(11) ROSENCRANCE, Linda. 11 Facebook Privacy Steps to Take Now. *SecurityNewsDaily* [online]. ©2018 [cit. 2018-04-27]. Dostupné z: http://www.technewsdaily.com/7832-11-facebook-privacy-steps.html

(12) DOČEKAL, Daniel. Facebook začíná mladé nudit, do čeho se vrhnou po něm. Lupa.cz [online]. ©2018 [cit. 2018-04-23]. Dostupné z: http://www.lupa.cz/clanky/facebook-zacina-mlade-nudit-do-ceho-se-vrhnou-po-nem/?labelsBox-labelId=97&do=labelsBox-switch

(13) Facebook v České republice. *Newsfeed* [online]. 2017 [cit. 2018-05-12]. Dostupné z: https://newsfeed.cz/cesky-facebook-v-q1-2017-hlasi-48-milionu-uzivatelu-mesicne/

(14) PROKŮPEK, V. Twitter: Historie, výhody a nevýhody. *In: Zive.cz* [online]. 2017 [cit. 2018-05-12] Dostupné z: http:// vaclavprokupek2012.blog.zive.cz/2012/05/twitter-historie-vyhody-a-nevyhody/

(15) Za deset let se stal YouTube druhou nejnavštěvovanější stránkou. *TELEVIZE, Česká.* [online]. [cit. 2018-04-19]. ČT24. Dostupné z: http://www.ceskatelevize.cz/ct24/media/1527110-za-deset-let-se-stal-youtube-druhou-nejnavstevovanejsi-strankou

(16) Informace o YouTube. *Wikipedie* [online]. [cit. 2018-05-09]. Dostupné z: https://cs.wikipedia.org/wiki/YouTube

(17) Instagram. Google Play [online]. [cit. 2018-04-21]. Dostupné z: https://play.google.com/store/apps/details?id=com.instagram.android

(18) VOJTĚCH, Petr. Instagram končí se čtvercovým formátem. Mobilenet.cz [online]. 2015 [cit. 2018-04-19]. Dostupné z: https://mobilenet.cz/clanky/instagramkonci-se-ctvercovym-formatem-28008

(19) Vincos Blog. The State of Linkedin. *vincos.it* [online]. ©2013 [cit. 2013-04-07]. Dostupné z: http://vincos.it/the-state-of-linkedin/

(20) Informace o společnosti Google. *Wikipedie* [online]. [cit. 2018-05-12]. Dostupné z: https://cs.wikipedia.org/wiki/Google

(21) Seznam spustil novou verzi Lide.cz. *Živě.cz* [online]. [cit. 2018-05-12]. Dostupné z: https://www.zive.cz/bleskovky/konecne-seznam-spustil-kompletne-predelany-web-lidecz/sc-4-a-173073/default.aspx

(22) Služby sociální sítě Libimseti.cz. *Libímseti.cz* [online]. [cit. 2018-05-12]. Dostupné z: http://napoveda.libimseti.cz/sluzby/moje-libimseti.html

(23) Spolužáci končí. *Technet* [online]. [cit. 2018-04-21]. Dostupné z: https://technet.idnes.cz/sluzba-spoluzaci-cz-konci-2018-dga-/sw_internet.aspx?c=A180404_125301_sw_internet_pka

(24) Podvod na Facebooku. Technet [online]. [cit. 2018-05-09]. Dostupné z: https://technet.idnes.cz/podvod-na-facebooku-0os-/kratkezpravy.aspx?c=A170726_ 132026_tec-kratke-zpravy_vse

(25) Obří skandál Facebooku. Echo24 [online]. [cit. 2018-05-09]. Dostupné z: https://echo24.cz/a/SMbyP/obri-skandal-facebooku-unik-osobnich-udaju-se-mohl-tykat-dvou-miliard-lidi

(26) Micro těžba kryptoměn, malware Facebooku. Technet [online]. [cit. 2018-05-09]. Dostupné z: https://technet.idnes.cz/trend-micro-tezba-krytpomena-facebook-messenger-digiminer-monero-kod-malware-188-/kratke-zpravy.aspx?c=A171228_ 095333_tec-kratke-zpravy_vse

(27) MENN, Joseph. Social networks scan for sexual predators, with uneven results. *Reuters* [online]. 2013 [cit. 2018-04-07]. Dostupné z: http://www.reuters.com/article/2012/07/12/us-usa-internet-predators-idUSBRE86B05G20120712

(28) LIEBOWITZ, Matt. Zombie Blondes Invade Facebook with Fake Profiles. *SecurityNewsDaily* [online]. 2013 [cit. 2018-04-07]. Dostupné z: http://www.securitynewsdaily.com/1889-zombie-blonde-facebook-fake-profile.html

(29) ISO/IEC 27035:2016. *Information technology — Security techniques — Information security incident management*. ISO. 2016. 53 s.

(30) ČSN ISO/IEC 27005. *Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací. Český normalizační institut*. 2008. 50 s.

SEZNAM TABULEK

SEZNAM OBRÁZKŮ