Bezpečnostní rizika internetových sociálních sítí

The security risks of internet social networks

Bc. Antonín Mrkva

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Antonín MRKVA**
Osobní číslo:	**A10502**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnostní rizika internetových sociálních sítí**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na dané téma.**
2. **Definujte pojem sociální síť a formulujte jeho charakteristiky a vliv na kriminalitu.**
3. **Proveďte analýzu bezpečnostních rizik u sociálních sítí budovaných v prostředí internetu.**
4. **Navrhněte konvence použití sociálních sítí koncovými uživateli, minimalizující riziko zneužití třetími osobami.**
5. **Ověřte použitelnost vytvořených konvencí v praxi.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **SARNECKI, Jerzy. Delinquent Networks. Youth Co-Offending in Stockholm. 1st printing, 2001. Cambridge University Press; London. 214 s. ISBN 978-0-521-80239-0.**
2. **BARABÁSI, Albert-László. V pavučině sítí. 1. vydání, 2005. Paseka; Praha. 280s. ISBN 0-262-08153-9.**
3. **JAISHANKAR, Karuppannan. Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. 1st printing, 2011. Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India. 461 s. ISBN 978-1-439-82949-3.**
4. **JIROVSKÝ, Václav. Kybernetická kriminalita. 1. vydání, 2007. Grada; Praha. 240s. ISBN 80-247-1561-9.**
5. **BUREŠ, L. Internetové sociální sítě, pohled na jejich využívání především žáky ZŠ a s tím spojená případná rizika. Brno, 2010. 83 s. Diplomová práce na Pedadgogické fakultě Masarykovy Univerzity na katedře technické a informační výchovy. Vedoucí diplomové práce Ing. Martin Dosedla.**
6. **Social network - Wikipedia. URL: (http://en.wikipedia.org/wiki/Social_network).**

Vedoucí diplomové práce: **Ing. Dalibor Slovák**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **28. února 2011**

Termín odevzdání diplomové práce: **17. října 2011**

Ve Zlíně dne 28. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce si klade za cíl analyzovat bezpečnostní rizika sociálních sítí budovaných v prostředí internetu, popsat důsledky jejich zneužití a navrhnout řešení v podobě konvencí, kterými by se měl uživatel internetové sociální sítě řídit pro co největší minimalizaci těchto rizik. Tyto portály totiž lidé nevyužívají jen k soukromým účelům, ale také pro obchodní komunikaci. Podniky dokonce implementují sociální sítě do svých informačních systémů a prohlubují tak možnosti komunikace se svými zákazníky. V rozhraní sociální sítě se jedná v obou případech o téměř nijak nechráněná data, která představují atraktivní cíl pro útočníky. Jedná se proto o velmi aktuální problém, který je potřeba řešit.

První část práce definuje pojem internetová sociální síť a podává jeho teoretické vysvětlení zahrnující také historií vzniku, současnost a pravděpodobnou budoucnost těchto sítí s ohledem na rostoucí globalizaci společnosti a s tím souvisejících nevýhod v podobě bezpečnostních rizik, které si uživatel většinou sám plně neuvědomuje. Druhá část práce analyzuje bezpečnostní rizika a jejich dopady na jednotlivce i společnost jako celek. Z důvodu rostoucí interakce uživatele s internetovou sociální sítí a neustálému vzniku nových trendů nelze popisovat jen aktuální problémy bez toho, aniž by tato práce a její řešení bylo aktuální i za několik let. Pro maximální objektivnost se proto práce zaměřuje především na informační bezpečnost a ochranu soukromí. Ve třetí části práce navrhuje konvence, kterými by se měli uživatelé komunitních webů řídit. Analýzou technologii využívaných na internetu můžeme tvrdit, že technologie samy o sobě nejsou nebezpečné, nebezpečný je lidský element. V případě dodržování předkládaných konvencí, z nichž většina je univerzálně platných při používání všech internetových služeb, bude riziko zneužití minimalizováno.

Klíčová slova: sociální síť, bezpečnostní riziko, soukromí, osobní údaj, internet

ABSTRACT

This thesis aims to analyze the security risks of social networks built on the internet, to describe the consequences of their abuse and to propose solutions in the form of conventions, which would give the user control the online social network for maximum minimize these risks, because people just do not use social networks for private purposes but also for business communications. Enterprises even implement social networking into their information systems and thus widening the possibilities of communication with their customers. The social network interface is in both cases by almost any unprotected data, which represent an attractive target for attackers. It is therefore a very topical issue that needs to be addressed.

The first part defines an Internet social network and gives his theoretical explanation involving the formation history, present and probable future of these networks with regard to the increasing globalization of society and the associated disadvantages in terms of security risks, which the user usually does not realize himself fully. The second part analyzes the security risks and their impact on individuals and society as a whole. Due to increasing user interaction with the Internet community networks and the constant emergence of new trends not only describe the current problems without it, without the work and the actual solution was even a few years. For maximum objectivity, therefore, the work focuses on information security and privacy. In the third part of the work proposed convention, which would allow users to manage community websites. Analysis of the technology used on the Internet, we can argue that technology itself is not dangerous, dangerous is the human element. In the case of compliance submitted to the convention, most of which are universally applicable for use of any Internet service, will minimize the risk of abuse.

Keywords: social network, security risks, privacy, personál data, intenet

Rád bych touto cestou poděkoval svému vedoucímu diplomové práce panu Ing. Daliboru Slovákovi, za jeho cenné připomínky, ochotu a trpělivost. Mé poděkování dále patří mé rodině, přátelům a známým za jejich podporu a trpělivost.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně ……

podpis diplomanta

OBSAH

ÚVOD

S rozvojem nových technologií roste přímo úměrně nebezpečí jejich zneužití vůči jejím uživatelům. Jednou z nejvíce rozvíjených platforem posledních desetiletí je bezpochyby internet, který jakožto převažující médium dnešní doby nabízí mnoho oblastí využití. V rámci internetu mohou uživatelé využívat mnoho služeb, především WWW, tedy systém webových stránek, které se zobrazují ve webovém prohlížeči. Popularita této služby neustále roste nejenom díky relativně jednoduchému a pro většinu obyvatelstva přístupnému prostředku pro sdílení informací a komunikaci, ale také díky vývoji nových trendů v závislosti na potřebách uživatelů. Jedním z trendů jsou sociální sítě, což je propojená skupina lidí, kteří se schází za účelem určité interakce. Může se jednat o kamarády, lidi se stejnými zálibami, a podobně. Sociální sítě již využívá desítky milionů lidí a jejich počet neustále roste. Již z podstaty interakce mezi dvěma a více počítači v síti internet vyplývá bezpečnostní riziko zneužití dat třetími stranami k různým účelům. Internet poskytuje určitou míru anonymity a pseudonymity, takže není zaručeno, že uživatel, s nímž komunikuje je ten, za kterého se vydává. Není také zaručena integrita dat (je možné data odposlouchávat a měnit, než se dostanou k cílovému uživateli). Rozhraní sociálních sítí navíc nepodporuje ve většině případů komunikaci přes kryptografické protokoly, které jsou zpravidla nasazovány pro komunikaci i s méně citlivými daty.

Nejedná se přitom jen o informační bezpečnost a ochranu soukromí, ale také další delikty, mezi které se řadí například kyberšikana, kybergrooming a kyberstalking. Těmto tématům je stále věnována poměrně malá pozornost, proto má smysl se o nich v této diplomové práci zmínit.

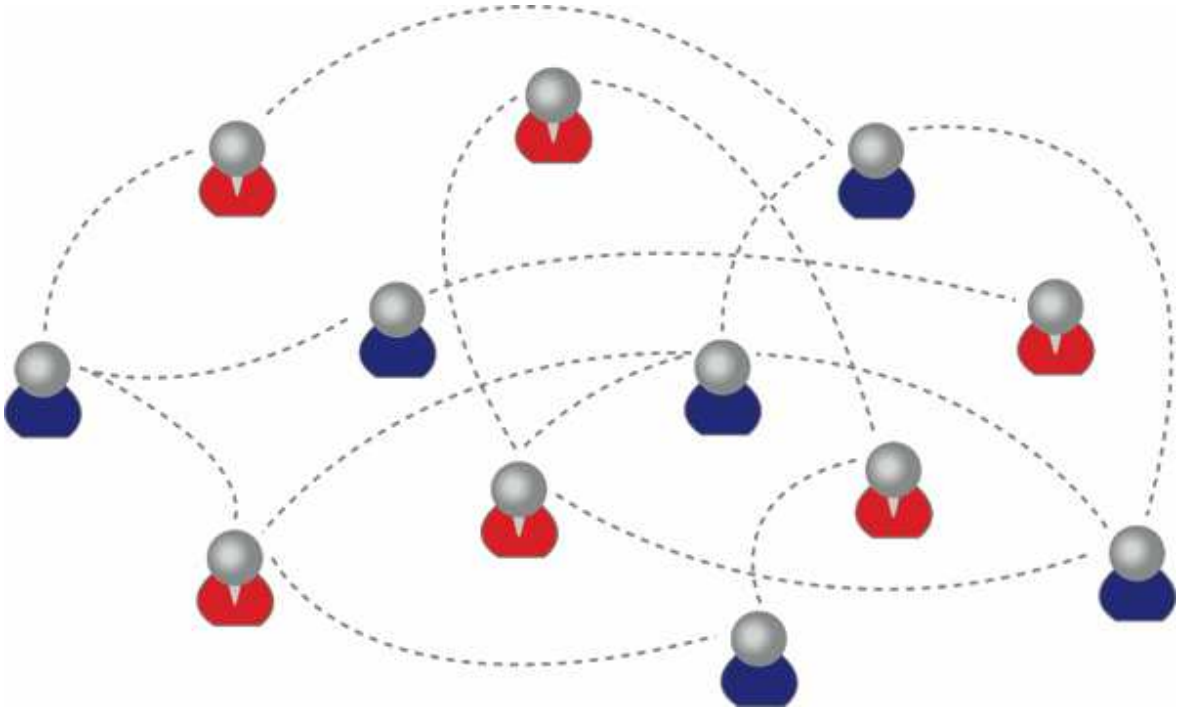
I. TEORETICKÁ ČÁST

SOCIÁLNÍ SÍŤĚ

1.1 Definice základních pojmů

1.1.1 Internetová sociální síť

Internetová sociální síť je webové rozhraní vytvořené za účelem sdílení informací různého charakteru mezi lidmi, kteří mají určitý vztah, vazby či společnou vlastnost. Mohou to být lidé se stejnými zájmy, rodinní příslušníci, známí, kamarádi ze školy, spolupracovníci, zpěváci, atd. Webový portál obvykle vyžaduje registraci uživatele s vyplněním osobních údajů různého rozsahu, které jsou nezbytné pro interakci entit mezi sebou. Registrace je typicky podmíněna souhlasem se všeobecnými podmínkami, které mohou vymezovat další restrikce.



Obr. 1. Schéma propojení vazeb mezi uživateli sociální sítě

1.1.2 Bezpečnostní riziko

Bezpečnostní riziko je míra nepříznivých dopadů, které hrozí subjektu v případě, že v systému nastane okolnost nebo situace, která může potenciálně umožnit třetí straně manipulovat s daty subjektu nebo se subjektem samotným. Zneužitím bezpečnostního rizika utrpí poškozený duševní či materiální škody. Existuje mnoho druhů bezpečnostních rizik, avšak v případě sociálních sítí je za většinu z nich zodpovědný svým nezodpovědným chováním sám uživatel.

1.2 Vznik a historie sociálních sítí

Vznik první sociální sítě na internetu není jednoduché vystopovat. I vznik samotného internetu je spojen s potřebou sdílet informace v rámci dvou a více počítačů umístěných v síti. Jednalo se především o prostředek předávání dat v univerzitním prostředí, resp. v rámci vědeckého výzkumu. Lze tedy tvrdit, že internet byl zpočátku sociální síť, která sdružovala uživatele mající určité vlastnosti a cíle. Ti si vyměňovali vzkazy zpočátku pomocí e-mailové komunikace a až do objevení IRC (popsáno v kapitole 1.2.2) neprobíhala v reálném čase. Vývoj dalších technologií a především pak publikace prvních internetových stránek se staly významným mezníkem ve vzniku internetových sociálních sítí, jak je známe dnes. Hlavní rozdíl mezi dnešní podobou internetu a sociální sítí je ten, že internet je jednou z technologií, kterou aplikace (sociální síť, komunitní web) v něm umístěná využívá ke svému fungování.

1.2.1 Emailová komunikace

E-mail (elektronická pošta) zajišťuje komunikaci, tedy odesílání, doručovaní a příjem zpráv, mezi různými počítači v sítí. Ze své podstaty byl e-mail zpočátku primárně určen jako prostředek pro komunikaci mezi dvěma uživateli (odesilatel a příjemce zprávy). Brzy byl však objeven potenciál e-mailových diskusních skupin a konferencí, kdy je zpráva odeslaná jedním uživatelem doručena všem ostatním uživatelům přihlášeným ve skupině. Komunikace neprobíhá v reálném čase a je tedy relativně pomalá.

1.2.2 IRC

Internet relay chat (IRC) je způsob komunikace v síti internet v reálném čase. Protokol byl navržen v roce 1988 finským studentem Jarko Ojkarinnen jako prostředek pro komunikaci mezi skupinami lidí (many to many). Podporovala však i soukromé zprávy (one to one). Lidé zde komunikují v tzv. kanálech, tedy virtuálních místnostech vytvořených uživateli sítě pomocí specializovaného programu (klient). Jeden uživatel může být současně připojen k více kanálům. Každý uživatel sítě IRC vystupuje pod pseudonymem svého vlastního uvážení, který však nesmí být používán jiným, právě připojeným uživatelem. Kanál v síti IRC není permanentní a po odpojení posledního uživatele z diskusní skupiny zaniká.

Ve své době sdružovalo IRC značnou část uživatelů internetu. Při svém vzniku však Finsko nedisponovalo zahraniční konektivitou a síť IRC byla dostupná pouze v rámci Technické Univerzity v Helsinkách. S rostoucí popularitou však proběhla expanze do dalších univerzit a síť se velmi rychle zvětšovala. S globalizací internetu proběhlo rozšíření do dalších států a IRC se stalo celosvětovým trendem. Díky neshodám o další směřování vývoje se jednotlivé servery postupně oddělovaly a tvořily nové sítě založené na principu IRC. Vzniklo tak velké množství dalších sítí, z nichž některé fungují dodnes.

Protokol IRC trpěl ve své podstatě mnoha bezpečnostními riziky, z nichž nejpodstatnější jsou:

- posílání hesla v nešifrované podobě
- komunikace je náchylná k snadnému odposlechu
- absence jednoznačné identifikace entity vede ke kolizím při užití stejných pseudonymů
- dlouhé odezvy mezi požadavkem a odpovědí serveru umožňují potencionálnímu útočníkovi snadnou cestu k odchytávání dat a jejich podvržení

Z důvodů bezpečnostních rizik a technologických omezení vznikl nový protokol SILC (Secure internet live conferencing), jehož topologie je stejná jako u IRC, avšak všechna

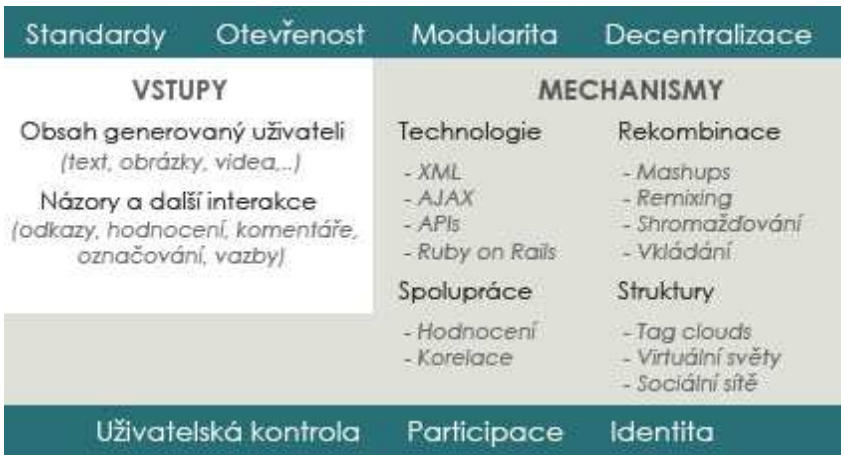
data jsou automaticky šifrována. Tento protokol lze tedy používat nejen pro účely textové komunikace, ale také k bezpečnějšímu posílání jakýchkoli jiných dat.

1.2.3 Webové rozhraní

Brzy po spuštění první webové prezentace a neustálému globálnímu rozšiřování internetu byl objeven potenciál webového rozhraní jakožto prostředku pro rychlou a snadnou komunikaci mezi lidmi odkudkoli, kde je možné se k internetu připojit. Prvním průkopníkem mezi sociálními sítěmi s webovým rozhraním se stal v roce 1995 web Classmates.com, který založil Randy Condards. Záměrem vytvářené sociální sítě bylo pomoci uživatelům navázat kontakty s přáteli z dob studia na základní, střední a vysoké škole. Potenciál tohoto konceptu byl dále využit pro setkávání spolupracovníků z práce a využití našel dokonce u armády Spojených Států Amerických. Web se stal velmi úspěšným a především myšlenka tvorby jednotlivých vztahů mezi uživateli se stala vzorem pro dnes nejznámější internetové sociální sítě.

1.2.4 Web 2.0

Termín web 2.0 je zavedené označení pro webové prezentace „nové generace“. Nejedná se přímo o novou technologii, ale o další etapu vývoje webu, v níž byl statický obsah nahrazen dynamicky se měnícím obsahem. Uživatel je zde obvykle motivován k činnosti, která garantuje decentralizaci autorit. Jedná se tedy o přesun centralizovaného přístupu tvorby obsahu na tvorbu ovlivněnou samotnými uživateli. Realizace vize web 2.0 probíhá formou specifických prvků, technologií a standardů využívající interakci uživatelů jakožto hlavní požadavek pro své fungování.



Obr. 2. Schéma technologií a prvků Web 2.0

1.2.4.1 Technologie, prvky a standardy Web 2.0

Jednou z těchto technologii a typický zástupce Web 2.0 je internetová sociální síť. Ta obvykle využívá nejširší spektrum funkcionalit, které uživatelům usnadňují vzájemnou interakci. Základním předpokladem aplikací vyhovujících standardu Web 2.0 je modulace, což zajišťuje implementaci nových funkcí, trendů a technologií na základě požadavků uživatelů. Ty jsou zpravidla do aplikací sociálních sítí integrovány ihned po svém uvedení a úspěšném otestování jejich funkčnosti. Často se můžeme setkat s kopírováním jednotlivých konceptů v rámci jednotlivých provozovatelů.

Web 2.0 zahrnuje následující prvky:

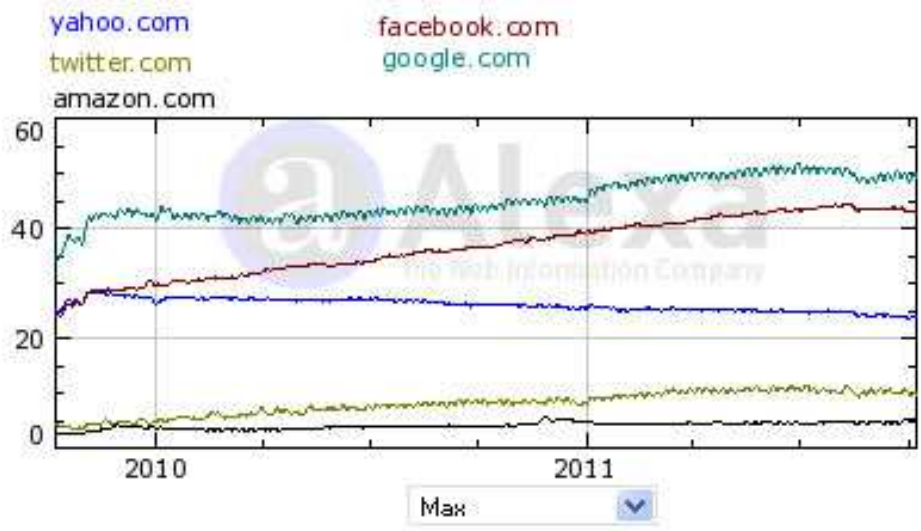
- **Funkcionalita –** kromě statického obsahu mající informační hodnotu je standardem do aplikací implementovat určitou funkcionalitu, která zajišťuje další funkce Web 2.0. Jedná se například o chaty, diskusní fóra a především pak sociální sítě, které integrují všechny funkce do jednoho celku.
- **Interakce –** uživatelé svým chováním vytvářejí prostředí aplikace a zajišťují neustálý přísun nového obsahu. Svou interakcí mohou tvořit personalizované prostředí, které se okamžitě přizpůsobí na základě jejich konání.
- **Dynamický obsah –** na utváření obsahu se svou interakcí podílejí všichni uživatelé sociální sítě. Z centralizované správy webu se tak stal systém decentralizovaný, který je v podstatě po obsahové stránce nezávislý na majiteli webu.
- **Sociální funkce –** spolu s registrací získá uživatel přístup do rozsáhlé virtuální společnosti, se kterou pak může komunikovat, hledat přátele, lidi se stejnými zájmy a podobně.

1.2.5 Budoucnost sociálních sítí

Sociální sítě se na internetu stávají spolu s vyhledáváním informací dominantní službou. Dá se předpokládat, že další postup ve vývoji webových technologií bude ve větší míře buď přímo integrován do sociálních sítí a dále přebírán dalšími službami nebo naopak. Není možné přesně předpovědět, jak bude další vývoj probíhat, avšak již nyní je možné dle nastupujících trendů odhadnout podobu internetových sociálních sítí v příštích letech.

S rozšiřujícími se technologiemi přímo úměrně rostou i možnosti aplikací, které je využívají. Sociální sítě se budou nadále rozvíjet o nové funkce a jejich význam bude růst.

Tento trend lze vysledovat prostým srovnáním návštěvnosti globálně nejpoužívanějších webů.



Obr. 3. Srovnání návštěvnosti

Z grafu[1] lze vyvodit, že zatímco sociální sítě facebook.com a twitter.com neustále zvyšují svůj podíl mezi uživateli internetu, zavedené projekty mají spíše sestupný či stagnující trend.

Dokonce i na televizních obrazovkách a dalších médiích se setkáváme se vzrůstajícím propojením se sociálními sítěmi. I hlavní zpravodajské relace často využívají jako svůj obrazový materiál videa ze serveru youtube.com a jemu podobných. Při rozhovorech v televizním studiu se stále častěji můžeme setkat s tím, že dotazy nepokládá moderátor, ale uživatelé sociální sítě. Mobilní telefon, který dokáže přistupovat k sociálním sítím, dnes již vlastní téměř každý. Stoupající vliv tedy nelze přehlížet a toto si uvědomují i vlastnící konkurenčních médií. A jak by mělo být u konkurenčního boje zvykem, těžit by z toho měl především uživatel.

[1] Trendy návštěvnosti spravuje monitorovací server Alexa.com.

„Zatímco dříve byly tradičně nejnavštěvovanějšími stránkami Internetu vyhledávače v čele s Google, nyní tyto přední pozice atakují sociální sítě Facebook a YouTube. Sociální sítě patří mezi tzv. technologie Web 2.0, tedy představují další vývojovou generaci Internetu v jeho struktuře a způsobu používání. Názory ohledně budoucnosti se různí, od silně favorizujících sociální sítě až po skeptické. Napovědět mohou pouze fakta: podle zprávy agentury Nielsen z roku 2010 tráví Američané nejvíce času (když jsou on-line) právě na sociálních sítích. Na druhém místě jsou on-line hry a teprve na třetím e-mail“ [4]

1.3 Způsoby využití

Využití internetových sociálních sítí je v současné době velmi široké a kromě soukromých osob a firem zabývající se informačními technologiemi zahrnuje i obory, které nemají s počítači a internetem nic společného. Důvodem pro tak široké využití je především přirozený zájem lidí mezi sebou jednoduše komunikovat a sdílet data různého charakteru. Přirozený zájem uživatelů registrovat se v internetové sociální síti ústí v obrovský marketingový potenciál, tedy možnost cíleně oslovit uživatele s určitými vlastnostmi splňující zadání reklamní kampaně. Tato práce si klade za cíl analyzovat bezpečnostní rizika a navrhnout konvence, které zaručují jejich minimalizaci. Jelikož základním článkem každé sociální sítě je uživatel, bude se práce kromě podkapitoly 1.3.2 z důvodu zvoleného tématu nadále zabývat pouze využitím sociálních sítí jako komunikačního prostředku mezi lidmi. Budeme zanedbávat jakýkoliv vliv marketingu a reklamních kampaní.

1.3.1 Komunikace a výměna dat

Jedním z podnětů pro vznik sociálních sítí na internetu byla snaha o zjednodušení komunikace a výměnu dat mezi lidmi z celého světa. Tato funkcionalita byla od začátku stěžejní záležitostí, avšak rozšířená o mnoho dalších služeb, které umožňují kromě již zmíněné komunikace například setkávání lidí a s tím související tvorba okruhů přátel a známých, s nimiž je možné prostřednictvím sociální sítě komunikovat. Důležitým předpokladem pro fungování sociální sítě je možnost modulace a snadného rozšíření aplikačního prostředí na základě požadavků komunity. Sociální sítě proto nabízí rozsáhlé možnosti pro komunikaci a výměnu dat. V podstatě všechny služby, kterými každá implementace sociální sítě disponuje, jsou ve své podstatě určeny ke komunikaci mezi

lidmi. Mezi stěžejní komunikační kanály patří chat, diskusní skupiny, a soukromé zprávy. Tyto služby jsou natolik samozřejmé, že se bez nich neobejde žádná implementace. Pro výměnu dat jiných než prostý text jsou často používány především přílohy, které by mělo jít ke každé odeslané zprávě připojit, stejně jako je to u e-mailových služeb. Pro výměnu obrázkových dat je dostačující funkcionalita fotogalerie.

1.3.2 Integrace do firemního informačního systému

Uživatelé sociální sítě pomocí vzájemné interakce přizpůsobují svůj profil tak, že je možné na ně velmi účinně cílit inzerci. Stále více společností integruje sociální sítě do svých CRM. Prohlubují tak možnosti komunikace se zákazníky a zároveň otevírají nové možnosti propagace a jejího řízení na internetu. CRM využívající sociální sítě, tedy SCRM (Social customer relationship management), znamená konkurenční výhodu ve smyslu rozvíjení a aktualizací dat přímo svými zákazníky. Najednou má firma přehled o tom, zda se zákazníkům líbí její výrobek a proč tomu tak je, respektive není. Tím však možnosti využití sociálních sítí obvykle nekončí. Pomocí příspěvků mohou uživatelé v sociální síti referovat své hlubší názory a pocity na daný výrobek či službu. Pro firmu tyto příspěvky znamenají reálné informace, které může využít při dalším rozhodování o strategiích do dalších období. Integrace sociální sítě do CRM nabízí firmě následující výhody:

- Bezplatné zviditelnění – založení profilu je obvykle zdarma a je prvním krokem ke zviditelnění společnosti na internetu. Jeho založením dá firma světu vědět o tom, co dělá, jaké jsou její cíle, případně poskytne odkaz na své webové stránky, a podobně.

- Kontakt se zákazníky – tím, že si uživatel sociální sítě přidá do svého okruhu vztahů danou firmu, se z něj stává potencionální zákazník, jelikož uvidí veškerou veřejnou komunikaci firmy v sociální síti. Na zprávy může dále reagovat svými dojmy a názory a tím poskytnout firmě cenné informace. Firma může formou zpráv uvádět novinky ve své produkci, akce, slevy, tiskové zprávy, atd.

- Reklama – všechny velké sociální sítě nabízí rozsáhlé možnosti cílení inzerce, např. dle demografie, pohlaví, věku, vzdělání a především pak zájmů. Firma tak může vytvořit vysoce cílenou reklamní kampaň pro propagaci svých produktů a služeb.

- Prodej – firmy mohou na sociální síti dokonce přímo prodávat své produkty a služby. Sociální síť Facebook pro tyto účely dokonce nabízí vlastní platební nástroj včetně platební brány, kterým lze za nabízené produkty platit.

1.3.3 Virtuální vizitka

Každá sociální síť vytvoří uživateli po registraci virtuální vizitku – profil, který obsahuje data různého charakteru. Profil může být buď veřejně přístupný všem uživatelům internetu nebo mohou být nastaveny restrikce umožňující přístup k profilu pouze autorizovaným osobám. Stejně jako vytvoření, i jeho následná úprava je jednoduchou záležitostí. Uživatel má obvykle naprostou kontrolu nad tím, co si na svůj profil umístí a bezprostředně po publikování mohou ostatní nahlížet na změny v reálném čase. Profily jsou hlavní devízou internetových sociálních sítí a jejich význam dále roste. Vzhledem k silné pozici ve vyhledávačích na ně v mnoha případech přistupuje více lidí, než na klasické internetové prezentace (blogy, osobní stránky, apod.) a profily na sociálních sítích tak stále nabývají na významu a stávají se nedílnou součástí prezentace mnoha lidí a firem na internetu.

1.3.4 Blogování a mikroblogování

Neexistuje jednoznačná formální definice výrazu blog. Termín blog je složeninou dvou anglických slov – web a log, z jejichž překladu vyplývá, že se jedná o webovou aplikaci uzpůsobenou pro publikační činnost. Tato aplikace může být spravována jedním či více editory, kteří publikují svou tvorbu pomocí příspěvků, které se následně zobrazují nejčastěji v obráceném chronologickém pořadí, tedy sestupně dle data vydání. Rozsah a zaměření blogu nabývá mnoha rozměrů a na internetu se s nimi běžně setkáváme, aniž bychom si to uvědomili. Mohou to být jednoduché webové deníky či zápisníky, firemní prezentace, ale také oficiální stránky zpravodajských serverů a podobně. Blog si může založit kdokoliv s přístupem k internetu, a to pomocí specializovaných webových serverů nebo instalací aplikace na vlastním serveru s využitím vlastní domény.

Termín „mikroblogování“ zachovává specifické vlastnosti blogování, avšak ve své nejsurovější podobě. Původním záměrem byla publikace krátkých textových příspěvků na internetu podobných SMS zprávám z mobilního telefonu. Proto je délka jedné zprávy omezena na 140-160 znaků. Od počátku bylo možné pomocí specializované SMS brány zveřejnit svůj příspěvek na internetu odesláním SMS zprávy s tímto příspěvkem. Tato koncepce je zachována dodnes, avšak bývá vytlačována publikací a čtením zpráv přímo přes PC. Nejznámější službou využívající „mikroblogování“ jako základní prvek pro své fungování je sociální síť Twitter, jíž je věnována kapitola 1.4.2. Také většina dalších

sociálních sítí obsahuje funkcionalitu „mikroblogování“, která se obvykle nazývá statusy, které mohou uživatelé neomezeně měnit.

1.4 Příklady sociálních sítí na internetu

1.4.1 Facebook

Facebook byl spuštěn v únoru 2004 studentem Harvard University Markem Zuckerbergem. Jedná se o nejpopulárnější internetovou sociální síť, která disponuje více než 650 miliony registrovaných uživatelů (tento údaj je aktuální k datu 7. března 2011). Původně byl koncipován jako sociální síť pouze pro studenty Harvardu, avšak po velmi krátké době se rozšířil i mezi další americké univerzity. Do srpna 2006 byla registrace umožněna pouze akademické obci a univerzitním studentům, tedy všem, kteří vlastnili e-mailovou adresu s koncovkou .edu, ac.uk, atd.. Nyní se může registrovat jakákoliv osoba starší 13 let.

Obr. 4. Logo sociální sítě Facebook

Registrace do aplikace Facebook je možná přímo z hlavní stránky a vyžaduje vyplnění základních osobních údajů:

- Jméno a příjmení
- E-mail
- Pohlaví
- Datum narození

Samozřejmostí je zvolení požadovaného hesla, na které však nejsou kladeny výraznější restrikce a je tak možné zadat i velice jednoduché heslo bez nutnosti současného využití písmen, číslic a dalších znaků. Po odeslání registračního formuláře je ještě nutné opsat z obrázku bezpečnostní kód, který brání robotům v automatických registracích.

Obr. 5. Registrační formulář sociální sítě Facebook

Platnost registrace není nutné dále ověřovat, např. pomocí e-mailu s aktivačním kódem. Ihned po registraci je uživateli nabídnut průvodce „Jak začít“, který umožňuje v prvním kroku hledání svých přátel a známých v uložených kontaktech e-mailové schránky. Tuto službu u nás podporuje například portál Seznam.cz. Dalším krokem je možnost vyplnění údajů o dosaženém vzdělání a informace o škole a zaměstnání. Posledním krokem je možnost nahrání profilové fotky – z počítače výběrem obrázku nebo vyfocením přes webovou kameru. Profilové foto se vždy zobrazí vedle jména a příjmení uživatele.

Obr. 6. Nahrání profilové fotky na sociální síť Facebook

Po úspěšném naplnění svého profilu základními informacemi může uživatel již bez omezení využívat všech služeb aplikace. Na hlavní stránce je zobrazena veškerá aktivita lidí, které má daný uživatel mezi přáteli. Mezi nejdůležitější a zároveň nejvyužívanější funkce patří:

- **Zeď –** souhrn všech aktivit daného uživatele.
- **Zprávy –** jedná se o soukromou korespondenci mezi daným uživatelem a jeho přáteli.
- **Události –** agenda obsahuje souhrn událostí, které vytvořil buď sám uživatel nebo jeho okolí.
- **Hledání přátel –** umožňuje na základě jména a příjmení najít konkrétního člověka na sociální síti.
- **Skupiny –** vytváření a správa skupin, do kterých se mohou následně přihlašovat jiní uživatelé. Skupiny mohou být uzavřené což znamená, že kdokoliv může zobrazit skupinu a její členy, ale pouze členové mohou zobrazit příspěvky. Dále pak otevřené (kdokoliv může zobrazit skupinu, její členy a příspěvky, které členové přidají) a tajné (pouze členové mohou zobrazit skupinu, její členy a příspěvky, které členové přidají).

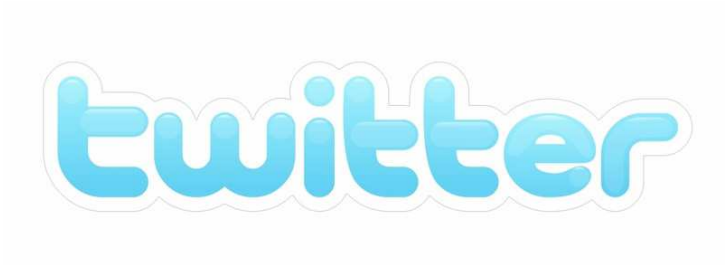
- **Aplikace –** tato agenda obsahuje veškeré aplikace, které uživatel využívá. Existuje nepřeberné množství aplikací, které lze využít. Mezi ty nejpoužívanější patří fotogalerie, poznámky a různé interaktivní hry.
- **Stránky –** zde je možné vytvářet a spravovat stránky, které mohou být různého charakteru. Jedná se například o cílené stránky k různým produktům a firmám, dále různá sdružení, zájmové skupiny nebo stránky známých osobností. Ke každé stránce je možné přiřadit různé aplikace, například diskusi a fotografie.

Hlavní stránka dále obsahuje výpis přátel spolu s miniaturou jejich profilové fotografie, návrhy lidí, které uživatel možná zná, cílenou reklamu a v horní části navigační menu.

Jedná se o nejnavštěvovanější sociální síť na světě.

1.4.2 Twitter

Twitter je služba nabízející svým uživatelům sociální síť a službu tzv. „mikroblogování“, tedy zasílání krátkých textových zpráv obsahujících maximálně 140 znaků, které se následně zobrazují v uživatelově veřejném profilu. Twitter byl založen v roce 2006 a díky jednoduchosti svého rozhraní a ovládání si brzy získal velkou oblibu. Nyní disponuje více než 200 miliony uživatelů z celého světa, kteří denně vygenerují přes 400 milionů krátkých textových zpráv a miliardu vyhledávacích dotazů.



Obr. 7. Logo sociální sítě Twitter

Velkým positivem je poskytování API, tedy rozhraní pro tvorbu dalších aplikací využívající sociální síť Twitter. Jedná se především o možnost integrace rozšířené funkcionality do vlastních webových či desktopových aplikací, které následně mohou při určité akci odesílat krátké textové zprávy do sítě Twitter a podstatně tak ulehčit práci s jejich publikací. Uživatelé Twitteru mají možnost kromě psaní na počítači zprávy zveřejňovat také pomocí odeslání SMS zprávy na specializovanou bránu. Mnoho

specializovaných internetových serverů také poskytuje zasílání aktuálních zpráv ze sociální sítě Twitter na e-mailovou schránku.

Twitter jako komunikační platformu využívá stále více lidí, přičemž komunikace probíhá na rozdíl od jiných služeb převážně veřejně. Dle statistik je Twitter nejrychleji rostoucí sociální sítí na internetu. Hlavním důvodem pro tak velký růst je pravděpodobně velké spektrum využití:

- **komunikace s přáteli**
- **zpravodajství a komentáře** – už i velké zpravodajské služby používají jako součást své publikační činnosti Twitter. Obvykle zveřejní titulek zprávy spolu s externím odkazem na celý článek a zajistí si tak kromě přílivu nových čtenářů i bezplatnou inzerci.
- **sledování uživatelů** – mnoho uživatelů využívá Twitter jako svou nástěnku pro veškerý svůj denní plán. Mezi nejčastěji navštěvované stránky se řadí například profily známých osobností, z nichž celá řada využívá Twitter jako prostředek pro vedení „veřejného deníku“.

1.4.3 MySpace

Mezi další velmi rozšířenou sociální síť můžeme zařadit Myspace. Jako jedna z prvních sociálních sítí si získala velkou popularitu, a to zejména v USA a dalších anglicky mluvících zemích. Byla založena v roce 2003 v Kalifornii na popud založení jiné sociální sítě s názvem Friendster. Několik zaměstnanců společnosti eUniverse si všimlo velkého potenciálu, integrovali několik dalších funkcí a nápadů a svůj projekt nazvali Myspace. Funkcionalita je obdobná jako u sociální sítě Facebook, tedy především vytvoření virtuálního prostoru pro setkávání přátel a známých. Tvorba vzájemných vazeb, komunikační a sociální funkce jako např. chatování, posílání zpráv, prohlížení fotografií a videí jsou základním pilířem fungování Myspace. Výhodou je možnost personalizace vzhledu profilu dle vlastního uvážení.

Obr. 8. Logo sítě Myspace

V roce 2005 byl Myspace odkoupen za 580 milionů dolarů společností News Corporation, kterou vlastní Rupert Murdoch. Myspace se až do roku 2008 držel dle analytické společnosti Alexa na prvním místě mezi sociálními sítěmi, ovšem byl překonán službou Facebook a poté dalšími sítěmi. Důvodem byla špatná strategie řízení webového portálu s minimem inovací, který měl oproti konkurenci zastaralé rozhraní i funkcionalitu. Proběhlo několik drastických a unáhlených změn v designu, což způsobilo další odliv uživatelů ke konkurenci. Nakonec situace došla tak daleko, že bylo 95% akcií prodáno společnosti Specific Media za 35 milionů dolarů.

1.4.4 LinkedIn

Specializovaná sociální síť, kde se setkávají profesionálové všech možných oborů a komunikují mezi sebou. Služba byla založena v prosinci roku 2002 a spuštěna v první třetině dalšího roku. V současné době je zde registrovaných více než 120 milionů uživatelů z více než 196 zemí. Služba je zaměřená na profesionály a podnikatele, kteří si zde vyměňují své zkušenosti a komunikují v rámci svých pracovních zájmů. Obecně se dá říci, že uživatelé LinkedIn jsou vzdělanější než uživatelé jakékoliv jiné sociální sítě. Z toho vyplývá určitá úroveň počítačové gramotnosti a s tím souvisí menší pravděpodobnost zneužití bezpečnostních rizik. Síť je s úspěchem používána jak malými firmami, tak i velkými korporacemi.

Obr. 9. Logo služby LinkedIn

Základním kamenem LinkedIn je tvorba profesních vazeb s jinými lidmi. Uživatel sítě může pozvat kohokoliv (nejčastěji své kolegy či další lidi ze svého oboru podnikání) a dokonce to ani nemusí být uživatelé sociální sítě. Seznam vazeb pak může být použit k různým účelům:

- usnadňuje hledání práce, nových zaměstnanců či pracovních a podnikatelských příležitostí
- zaměstnavatelé mohou zveřejnit nabídky práce
- uživatelé mohou publikovat své fotografie a nahlížet na fotografie jiných, což usnadňuje identifikaci
- je možnost uložit zajímavé nabídky práce do zvláštní agendy
- lidé, kteří hledají práci, mají možnost kontaktovat manažery firem
- síť umožňuje také kontakt s lidmi, kteří nejsou přímo v seznamu vazeb a pro tyto účely nabízí vazby druhé a třetí úrovně. To si lze představit jako „známý mého známého“, respektive „známý známého mého známého“.

Registrace do sociální sítě je jednoduchá a vyžaduje pouze základní údaje. Jedná se konkrétně o celé jméno a příjmení, e-mail, heslo (musí obsahovat minimálně 6 znaků). Dále pak je potřeba vyplnit aktuální zaměstnání a pozici ve firmě a národnost. Průvodce registrací je jednoduchý a přehledný a nabízí i procházení kontaktů v zadané e-mailové schránce nebo odeslání pozvánek zvoleným uživatelům.

Existují dva typy členství. Základní je zdarma a obsahuje nezbytné funkce pro správu vazeb a svého profilu. Placený tarif pak obsahuje další funkce, jako například zobrazení informací o profilu uživatelů mimo seznam vazeb, více možností třídění, pokročilé vyhledávání a v neposlední řadě možnost kontaktovat všech více než 120 milionů uživatelů sítě.

Společnost provozující sociální síť LinkedIn vstoupila v květnu 2011 na burzu. *„LinkedIn se rozhodl emitovat akcie ve jmenovité výši 45 amerických dolarů, které se ve čtvrtek 19. května 2011 začaly obchodovat na americké burze NYSE.“* [6]

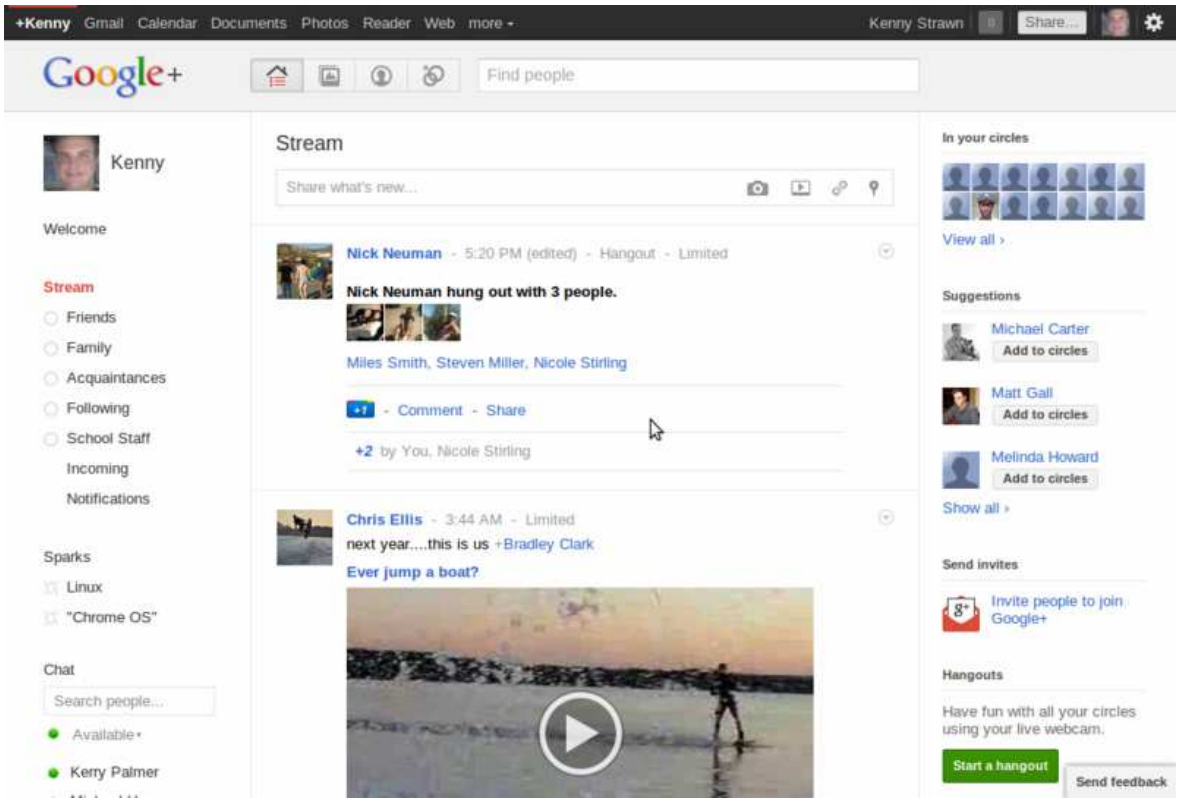
1.4.5 Google Plus

Google Plus (Google+) je novou sociální sítí, kterou provozuje a vyvíjí společnost Google. Vzhledem k boji o dominantní pozici na trhu společností působících na internetu bylo její spuštění logický krok. Síť byla spuštěna 28. června 2011 do fáze testování, kdy registrace byla možná jen na pozvánku, a to pouze pro uživatele starší 18 let. Toto opatření bylo zavedeno pravděpodobně proto, že Google ve fázi testování nebyl schopen zaručit ochranu osobních údajů dětí a dospívajících. Zájem o možnost registrace na pozvánku byl tak velký, že následující den byly pozastaveny. Následně bylo každému uživateli umožněno rozeslat pozvánku až 150 lidem. 20. září byla tato restrikce odstraněna a nyní se může do sítě registrovat každá osoba starší 13 let.

Obr. 10. Logo sociální sítě Google+

Filozofie této sociální sítě je založena na napodobení sdílení informací stejně jako v reálném životě. Tato myšlenka spočívá především v možnosti kontrolovat veškerou svou činnost ve společnosti, kdy se může člověk svobodně rozhodnout, komu poskytne které informace a za jakých podmínek. Funkce se jmenuje „Kruhy“ a dovoluje uživateli tvořit si seznamy lidí, kdy každému kruhu přiřadí různá práva. Je tak skutečně zajištěna kontrola nad přístupem ke svým datům, která respektuje přání svých uživatelů, stejně jako je to v reálném životě.

Google do své sociální sítě integroval i své další služby, Google Profiles [2]a Google Buzz[3]. Jako celek tvoří novou aplikaci, která má potenciál již od počátku konkurovat zavedeným značkám jako je Facebook či Twitter.



Obr. 11. Hlavní stránka sociální sítě Google+

Základní rozhraní je podobné vzhledu sociální sítě Facebook. Nabízí přehled o všech funkcích a poslední aktivitě přátel. Je však nutno zdůraznit absenci jakýchkoliv reklam.

[2] Nástroj pro prezentování své osoby na internetu.

[3] Nástroj pro tvorbu „mikroblogů“ a sdílení informací různého charakteru.

1.4.6 Lidé.cz

Lidé.cz je česká sociální síť provozovaná portálem Seznam.cz, v rámci jehož služeb je sjednocen přístup pomocí jednoho uživatelského jména a hesla. Uživatelé tak mají ihned po registraci do jakékoliv služby Seznam.cz přístup také do sociální sítě Lide.cz.

Obr. 12. Logo Lidé.cz

Sociální síť nabízí profily, vyhledávání lidí dle zadaných kritérií, diskuzi, seznamku, chat, možnost tvorby blogů a zprostředkuje také další externí služby, jako například online jazykové kurzy. Služba byla spuštěna v roce 1997, tedy dříve než konkurenční sociální sítě, měla tedy výhodu dominantního postavení na trhu. Zpočátku se služba zaměřovala na vyhledávání e-mailových adres. V roce 2004 byl zakoupen majoritní podíl v projektu Spolužáci.cz, který byl záhy připojen jako doplněk k Lide.cz. V roce 2008 pak proběhla celková proměna koncepce a modernizace vzhledu. Na hlavní stránce je velký prostor věnován představením vybraných profilů spolu s možností jednoduchého vyhledávání mezi uživateli sítě a dále pak souhrn všech služeb (diskuze, seznamka, apod.).

Nyní má služba více než milion registrovaných profilů, avšak počet skutečných uživatelů je menší, jelikož mnoho z nich má registrován více než jeden profil. Mezi uživateli převažuje mladší generace od 15 do 25 let. Lide.cz je tzv. otevřená síť, je tedy možné prohlížet si profily uživatelů bez nutnosti registrace. Je však možné blíže specifikovat, které informace a fotografie chce ten který uživatel zveřejnit.

Seznam.cz uvádí na svých stránkách také souhrnné statistiky služby Lide.cz:

Průměrná denní návštěvnost (RU): *	**236 337**
Měsíční počet zobrazených stránek (PV):	**412 651 548**
Průměrný čas strávený uživatelem na serveru (ATS): **	**3:30:44**
Struktura pohlaví: ***	**50% muži, 50% ženy**

* Průměr ze všech pracovních dnů ve sledovaném měsíci
** Vyjadřuje strávený čas uživatele za celý sledovaný měsíc
*** Průměrné rozložení populace ze všech celých týdnů ve sledovaném měsíci
Zdroj: Netmonitor.cz - SPIR - Mediaresearch & Gemius, Joint Panel, 15-day cookies, Červen 2011

Obr. 13. Statistiky portálu Lidé.cz

1.4.7 Spolužáci.cz

Spolužáci.cz je jedním z nejstarších tuzemských komunitních webů a již od svého založení se těší velké oblibě. Jeho koncepce je zaměřena na setkávání spolužáků, a to jak právě studujících, tak i absolventů. Jsou zahrnuty všechny stupně vzdělání kromě vysokých škol, tedy od základních po střední školy a učiliště. Další členění je realizováno formou vytváření jednotlivých tříd jednotlivých škol a následném přihlašování žáků do těchto tříd. Následně pak spolužáci v rámci třídy mohou mezi sebou komunikovat a vyměňovat data.

Obr. 14. Hlavní stránka projektu Spolužáci.cz

V roce 2004 koupila projekt společnost Seznam.cz, která jej začlenila mezi své služby. Byl kompletně modernizován vzhled, avšak koncept zůstal stejný. Každá škola má třídy, kterým je po vytvoření přidělen identifikátor (ID), pomocí kterého je možné ke třídě snadno přistupovat bez zdlouhavého hledání. Školy jsou rozděleny do měst a obcí, kde se nachází, následuje další členění do okresů. Pokud uživatel hledá konkrétní třídu, nejsnazší cestou, pokud zná ID třídy, je použití vyhledávacího formuláře. Další variantou je vyhledání požadované školy v hierarchiích okresů a měst. Pokud chceme vyhledat konkrétního spolužáka, k tomuto účelu slouží další vyhledávácí formulář, kde je možné zadat jméno, příjmení, okres a rok ukončení.

Každá třída má svého správce, který má na starost administrativní správu dané třídy spolužáků. Jeho úkolem je například schvalování žádostí o vstup do třídy či určení kontrolní otázky, jejímž prostřednictvím je po správném zodpovězení umožněn vstup do třídy.

Seznam.cz uvádí stejně jako u každé své služby také souhrnné statistiky.

Průměrná denní návštěvnost (RU): *	**101 514**
Měsíční počet zobrazených stránek (PV):	**43 868 774**
Průměrný čas strávený uživatelem na serveru (ATS): **	**0:21:46**
Struktura pohlaví: ***	**44% muži, 56% ženy**

* Průměr ze všech pracovních dnů ve sledovaném měsíci
** Vyjadřuje strávený čas uživatele za celý sledovaný měsíc
*** Průměrné rozložení populace ze všech celých týdnů ve sledovaném měsíci
Zdroj: Netmonitor.cz - SPIR - Mediaresearch & Gemius, Joint Panel, 15-day cookies, Červen 2011

Obr. 15. Statisitky projektu Spolužáci.cz

1.4.8 Líbímseti.cz

Líbímseti.cz je další z řady českých sociálních sítí, které se primárně zaměřují na vytvoření profilu a následné využití možností seznámení s jinými lidmi. Primární funkcí je tedy především seznamka, avšak stejně jako konkurenční síť Lidé.cz nabízí také další běžné služby, jako je například diskuze, hodnocení fotografií a chat. Navíc je možné využít funkce videochat, který jak již z názvu vyplývá, umožňuje kromě funkcí klasického chatu také vidět komunikující strany webovou kamerou. Princip seznámení s jiným uživatelem je koncipován maximálně zjednodušenou formou. K projevení zájmu o kontakt stačí pouze

jedno kliknutí myši. Vytvoří se tak potencionální pár, pro jehož aktivaci je nutné potvrzení od druhého uživatele. Tomu je při přihlášení oznámena skutečnost, že někdo jiný projevil zájem se s ním seznámit. Toto oznámení může buď ignorovat nebo schválit. Ve druhém případě bude potencionální pár aktivován, tedy umístěn do agendy „hotové páry“ a uživatelé spolu mohou dále dle libosti komunikovat.

Obr. 16. Logo Líbímseti.cz

Portál Líbímseti.cz vznikl v roce 2002 a těšil se velké oblibě hlavně mezi mladší generací. Spolu s Lidé.cz patřil mezi nejnavštěvovanější české sociální sítě. To však již dnes neplatí, jelikož oba portály v posledních letech překonal Facebook. V roce 2010 byl portál Líbímseti.cz prodán neznámým investorům.

II. PRAKTICKÁ ČÁST

2 ANALÝZA BEZPEČNOSTNÍCH RIZIK

Sociální sítě a především jejich používaní s sebou přináší mnohá bezpečnostní rizika, která mohou být zneužita. Podobně jako u jiných technologií, sociální sítě by bez interaktivních entit byly k ničemu. Právě lidský činitel a jeho chování v sociálních sítích určuje míru potencionálního rizika zneužití. Za posledních několik let se sociální sítě staly nedílnou součástí internetu a používá je stále více uživatelů. Bohužel, trendy se šíří v tomto případě podstatně rychleji, než informovanost o rizicích, která uživatelé jejich užíváním podstupují. Ohroženy jsou přitom všechny věkové skupiny, především pak děti a dospívající generace, která u obrazovek počítače tráví stále více svého času. Sociální sítě jsou koncipovány, jak již z názvu vyplývá, pro setkávání lidí a jejich vzájemnou interakci. Dá se tedy říci, že mnoho z nich hledá na sociální síti úprk od reality a žije zde svůj druhý život. Nejrizikovější skupinou se sklony k tomuto chování je opět nejmladší generace.

Nejedná se však pouze o problém závislosti na sociálních sítích. Pro motivaci k dalšímu čtení a snazší pochopení kořenů a příčin nejčastěji zneužívaných bezpečnostních rizik je sepsána kapitola „Motivace – nejčastější scénáře zneužití sociální sítě“. Tato kapitola obsahuje různé smyšlené scénáře z reálného světa, z nichž většina je aplikovatelná na téměř každého uživatele. Mnoho čtenářů si po jejich přečtení pravděpodobně uvědomí, že některé z popisovaných rizik se týká i jich. Následující kapitoly pak analyzují a popisují bezpečnostní rizika detailněji, včetně definice každého z nich.

Jak ukázal průzkum na stránkách Technet.cz, především mladí uživatelé sociálních sítí v ČR si nedostatečně hlídají své soukromí. *„Vystavují se riziku šmírování, a v případě, že zveřejňují citlivé osobní údaje, i vážnějším hrozbám. Plných šedesát procent náhodně vybraných uživatelů Facebooku naletělo na falešný profil neexistující dívky a přidalo si ji mezi přátele. Na neexistujícího mladíka se nachytalo 42 procent. Většina nachytaných pustila vetřelce ke všem datům, které přes Facebook prezentují: soukromé fotografie, fotografie přátel, e-mail, telefon, školu a v několika případech dokonce celou domovní adresu.“* [18]

V případě sociálních sítí dále platí pravidlo, že čím více uživatelů v jedné síti vystupuje, tím vyšší je riziko zneužití bezpečnostních rizik, kterými konkrétní implementace disponuje. Nejmladší generace se zde navíc setkává s mnoha různými názory a emocemi, které mohou ovlivnit jejich jednání. I z tohoto úhlu pohledu lze sociální sítě vidět jako velmi rizikové.

Díky potencionálně skryté identitě uživatelů na internetu, tedy i na sociální síti, nemůže komunikace probíhat stejně jako v reálném světě. Uživatelé si mohou svou komunikaci cíleně promyslet a předem připravit různé scénáře pro připravovaný rozhovor. Prostředí sociální sítě je mnohými lidmi zneužíváno k nevhodnému chování a dokonce kriminálním činům - a to vše bez toho, aby byla odhalena jejich identita. Vzhledem k tomu je potřeba jasně rozpoznat, definovat a popsat bezpečnostní rizika, kterým jsou uživatelé sociální sítě vystavováni.

2.1 Motivace – nejčastější scénáře zneužití sociální sítě

2.1.1 Pozvánka pro zloděje

Předpokládejme uživatele X, který má ve svém okruhu spoustu přátel a známých, řekněme více než 1000. Je mu 14 let, chodí na základní školu a jeho rodiče právě plánují dovolenou. Jelikož se uživatel X rád chlubí svým přátelům, neopomene ani tuto událost a napíše do sociální sítě vzkaz, že se už těší na dovolenou, která bude v období od 10. do 20. srpna. Tento vzkaz se následně zobrazí, v lepším případě, pouze všem jeho „známým“, které má uložené mezi svými přáteli a kteří tedy mají přístup k jeho datům včetně zmiňované zprávy. Uživatel X s rodiči odjede na dovolenou a jejich dům po dobu dovolené nikdo nehlídá. Po návratu bohužel zjistí, že jejich dům byl vykraden.

2.1.2 Falešný přítel

Uživatel X sociální sítě Facebook si tvoří okruh svých známých a přátel, se kterými by rád sdílel některá svá data včetně fotografií. Jelikož má uživatel X nastaveno schvalování požadavků o přátelství, má pak kontrolu nad tím, zda neposkytuje svá osobní data jiným lidem, než sám požaduje. Žádost a přidání mezi přátele mu poslala také Jana Nováková, která však nemá ve svém profilu vyplněna další data pro její jednoznačnou identifikaci a dokonce ani profilovou fotografii. Jelikož však shodou okolností byla Jana Nováková spolužačkou uživatele X, ten žádost o přátelství schválí. Později nalezne ve své e-mailové schránce nepřeberné množství nevyžádané pošty a dokonce mu volalo několik neznámých čísel. Jana Nováková nebyla tím člověkem, za kterého ji uživatel X měl. Udělením přístupu na soukromý profil však měl člověk skrytý za tímto profilem možnost získat citlivé osobní údaje a následně je zneužít k vlastnímu prospěchu.

2.1.3 Komunikace bez zábran

Slečně Janě je 17 let a sociální síť Facebook používá kromě komunikace také k seznamování se s novými kamarády. Na jednoho takového právě narazila. Důvěřivá a naivní dívka se postupem času začala svému virtuálnímu příteli svěřovat se svými tajemstvími, která by osobně neřekla ani svým největším kamarádkám. Virtuální přítel se jevil jako velmi ochotný a chápavý člověk a Jana si k němu vybudovala vztah. Přesto, že dotyčného osobně neznala a nikdy jej neviděla, zašle mu své, některé poněkud odvážnější fotografie. Virtuální přítel však namísto další komunikace a odhalení své identity začne Janu vydírat, že pokud se s ním nesetká, zašle fotografie do školy a jejím rodičům. Vystrašená dívka, aniž by se se svým problémem svěřila rodině, může následný stres a strach vyřešit mnohdy velmi radikálním způsobem.

2.1.4 Zničená kariéra

Pan Ondřej je studentem na univerzitě a uchází se o velmi lukrativní zaměstnání u jedné z partnerských firem této univerzity. Ondřej právě úspěšně dokončil praktickou část své diplomové práce a spolu se svými přáteli a spolužáky domluví oslavu této významné události. Bujarý večírek je v plném proudu a vzhledem ke stále se zdokonalující se technice mobilních telefonů je na večírku pořízeno nepřeberné množství fotografií, které jejich dotyční majitelé následně umístí na své veřejné profily na sociální síť. Ondřej je zde zobrazen v podnapilém stavu a kromě fotografií bylo také zveřejněno video, na kterém si utahuje ze svého budoucího potencionálního zaměstnavatele. Vzhledem k těmto materiálům pak Ondřej svou práci sice úspěšně obhájí, ale na lukrativní post je přijat někdo jiný.

2.2 Rozdělení bezpečnostních rizik

Bezpečnostní rizika lze pro snadnější klasifikaci členit hned několika způsoby:

- Míra poškození uživatele
    - Malá
    - Střední
    - Velká
- Důsledky zneužití
    - Osobní
    - Psychické
    - Majetkové
- Cílová skupina
    - Jednotlivec
    - Skupina
    - Instituce
    - Stát

2.3 Soukromí uživatele

Ochrana soukromí je v různém rozsahu skloňována a časována při práci člověka s jakýmkoli médiem, včetně internetu a technologií s ním souvisejících. Aniž by si to lidé uvědomovali, vlivem globalizace, vznikem nových komunikačních trendů a především samotnou podstatou globální počítačové sítě je soukromí uživatelů stále více narušováno různými vlivy. Bohužel, na internetu není možné se v žádném případě spoléhat na ochranu svého soukromí, jelikož i při pouhém prohlížení webových stránek, bez zadávání jakýchkoli dat pomocí klávesnice či myši, může být uživatel jednoznačně identifikován vhodnou implementací na straně serveru. Více informací o těchto technikách a možností jejich zneužití naleznete v kapitole 2.3.1.

2.3.1 Data odesílaná prohlížečem

Každý uživatel přistupující k síti internet má jednoznačně definovanou IP adresu, pod kterou jeho počítač v síti vystupuje. Pro prohlížení internetových stránek je nezbytný speciální software - webový prohlížeč (Mozilla Firefox, Internet Explorer, Google Chrome, atd.). Princip přístupu k webovým stránkám je v každém prohlížeči pouze otázkou implementace, avšak princip je stejný. Po zadání adresy webové stránky je odeslán požadavek na vzdálený server, který pak vrátí odpověď ve formě dat, která jsou zpracována prohlížečem. Data odeslaná prohlížečem do sítě internet však obsahují kromě nezbytných parametrů mnoho dalších informací, díky kterým lze uživatele jednoznačně identifikovat a přizpůsobit se tak jeho chování na tom kterém serveru. Při vhodné implementaci je v podstatě možné vést si o každém uživateli podrobnou agendu jeho chování. Toho je obzvláště využíváno například při cílení reklamy, jelikož ta se zobrazí jen těm lidem, kteří nějakým způsobem projevili zájem tím, že například hledali informace či četli článek o určitém tématu.

V případě internetových sociálních sítí nutnost jednoznačné identifikace uživatele dle dat odesílaných prohlížečem není většinou nutná. Přístup k ní má totiž většinou pouze registrovaný uživatel. Trasování je tak záležitostí pouhé interakce každého uživatele v síti.

Riziko zneužití těchto dat je však nízké. Vzhledem k povaze posbíraných dat lze například zpětně zjistit, o co uživatel při prohlížení sociální sítě projevil zájem a na tuto skutečnost dále reagovat zobrazením vhodně cílené reklamy. Využití pro vymezené interní účely je tedy přípustné a je také ošetřeno v podmínkách použití služby, se kterými uživatel při registraci do sociální sítě souhlasil. Problém nastává v případě úniku těchto dat třetím osobám. Zveřejnění některých atributů chování konkrétního uživatele může být citlivou záležitostí v osobním životě a v konečném důsledku může způsobit problémy až odloučení od společnosti.

2.3.2 Soukromí na sociálních sítích

Vzhledem k povaze sociální sítě je soukromí velmi problematickou záležitostí, protože nemůže být žádným způsobem zaručeno a při vytvoření profilu s implicitním nastavením, které většina uživatelů nemění je míra soukromí skutečně mizivá. Vše můžeme ilustrovat na sociální sítí Facebook, kde bez explicitního zásahu do funkce nastavení soukromí, o které většina uživatelů nemá ani tušení ani se ji nikdy nepokoušela hledat, se na sociální síti zobrazuje veškerá aktivita uživatele, takže každý může vidět, co jste právě kam napsali a vložili, co jste přidali či upravili atd. Nedá se tedy v žádném případě mluvit o soukromí.

„Soukromí je schopnost jedince nebo organizace kontrolovat shromažďování, ukládání, sdílení a přenos osobních informací a informací firemních. V obecném pojetí je právem jedince možnost kontroly informací o sobě a o své činnosti, spolu s ochranou proti nežádoucímu rušení. Termín soukromí (informační soukromí) se používá nejčastěji pro neformální motivaci k zajištění ochrany osobních informací, pravidel pro jejich kontrolu a poskytování jiným subjektům atd. Příklady relevantních bezpečnostních funkcí: anonymita, pseudonymita, nespojitelnost a nepozorovatelnost. Ochrana informačního soukromí nebo jen osobních dat může být důvodem pro zajištění bezpečnosti, stejně jako třeba ochrana firemních dat nebo informací vojenské rozvědky. V žádném případě nelze pojmy bezpečnost a informační soukromí volně zaměňovat, ale ani oddělovat. V ČR je vyjádřením práva na soukromí mimo jiné Zákon na ochranu osobních dat v informačních systémech.“ [1]

Jak je vidět z pohledu hlubší analýzy, žádná uvažovaná sociální síť uvedená v přehledu současně nesplňuje více než jednu bezpečnostní funkci. Některé aplikace sice dovolují nastavit pseudonym, pod kterým pak uživatel vystupuje, avšak pokud je spolu s tím vyžadováno celé jméno, funkce již z definice nemůže platit. Nespojitelnost je z důvodu odesílání dat prohlížečem a možnosti ukládání textových souborů do počítače irelevantní. Nepozorovatelnost může být za určitých okolností možná, avšak z definice vyplývá skutečnost, že využití zdrojů nemůže být pozorováno žádnou entitou včetně administrátora. Tato bezpečnostní funkce tedy také zjevně neplatí. Vzhledem k těmto skutečnostem můžeme tedy konstatovat, že soukromí na sociálních sítích neexistuje.

2.4 Internetová šikana

Internetová šikana (cyberbullying nebo kyberšikana) je druh útoku s dopadem na psychiku člověka, kdy útočník ke svému jednání využívá internet a jiné elektronické technologie a

prostředky (mobilní telefony, atd.). Tento druh šikany má své specifické znaky, kterými se liší od osobního kontaktu.

- **Útočník vystupuje anonymně**

I když je vystupování na sociálních sítích podmíněno registrací, toto opatření v žádném případě nezabrání využívat cizí identitu. Tato vlastnost sociálních sítí je velkou nevýhodou a pro běžného uživatele v podstatě neexistuje metoda pro odhalení pravé identity útočníka.

- **Útočník často mění místa, odkud útok provádí**

Specifické chování útočníků zahrnuje také častou změnu místa, odkud je jejich útok veden. Jelikož mnoho počítačů připojených k sítí internet využívá sdílenou IP adresu, je jejich identifikace o to složitější a vyžaduje spolupráci poskytovatele internetového připojení. I tak však úspěšnost identifikace pachatele je otázkou náhody. Navíc, pokud útočník vede útok pokaždé z jiného počítače, možnost jeho dopadení rapidně klesá.

- **Útoky probíhají většinou beze svědků**

Fyzické a psychické útoky vedené osobně mívají obvykle svědky v podobě například spolužáků či jiných přihlížejících osob. Následné usvědčení útočníka je tedy usnadněno případnou spoluprácí těchto lidí. Na internetu však každý uživatel zpravidla vystupuje jako jednotlivec a pokud se se svým problémem nesvěří okolí, jeho rozpoznání je otázkou náhody a mnohdy přijde příliš pozdě.

- **Může probíhat neúmyslně**

Díky absenci osobního kontaktu a z toho vyplívajícího rozeznání emocí a tónu hlasu je při komunikaci přes internet určitá pravděpodobnost, že si některá z komunikujících stran špatně vyloží poznámku, která byla myšlena odlišným způsobem. Ze špatně podaného vtipu tak může teoreticky vzniknout nedorozumění, jehož důsledkem je další rozkol. Neúmyslná šikana může nastat také tehdy, jestliže jsou zveřejněna data, která nějakým způsobem poškozují oběť, avšak jejich zveřejnění je myšleno jako vtip. První zdokumentovaný případ, kdy zveřejnění videa na sociální sítí vyústilo v těžkou psychickou poruchu poškozeného a bylo nutné podstoupit náročnou léčbu, je popsán v kapitole 2.4.1 Případ „Star Wars Kid“.

Obr. 17. Modelová představa internetové šikany

Projevy internetové šikany mohou být považovány za kriminální činy. Motivem fyzické i psychické šikany bývá nejčastěji pocit nadvlády útočníka nad svou obětí. Stejně je tomu i u šikany prováděné přes sociální sítě. Často je fyzická šikana doplněna právě internetovou šikanou, kdy je například natočeno video a to následně umístěno na sociální síť, což umocní dopad na psychickou stránku oběti. Jmenovaný příklad šikany se řadí mezi nejnebezpečnější, neboť zveřejnění videa na sociální síti je v podstatě nevratným činem a pokud se jedná o mimořádně ponižující událost, trauma a utrpení oběti bývá nesrovnatelně vyšší a často končí tragicky. Motivem útočníka či skupiny útočníků obvykle není majetek či peníze, i když i ty mohou být po oběti přímo vyžadovány. Vzhledem k anonymitě útočníka a nemožnosti včasné identifikace probíhající šikany od okolí není možné útočníka snadno identifikovat. Problém internetové šikany se tak v globálním měřítku řadí k jednomu z nejnebezpečnějších deliktů.

2.4.1 Případ „Star Wars kid“

Prvním zdokumentovaným a celosvětově známým případem internetové šikany bylo zveřejnění videonahrávky jistého kanadského studenta střední školy jménem Ghyslain Raza, který sám sebe v roce 2002 natočil videokamerou při nepříliš zdařilém ztvárnění své oblíbené filmové postavy z filmu Star Wars (odtud název „Star Wars kid“, tedy „kluk ze Star Wars“). Chlapec jako imitaci populární fiktivní zbraně „světelný meč“ použil golfovou hůl. Tato nahrávka se o rok později dostala do rukou jeho spolužákům, kteří ji následně umístili na internet pod názvem *Jackass_starwars_funny.wmv*. Nevinný kanadský žert se však změnil v katastrofu, jelikož video za poměrně krátkou dobu shlédlo několik milionů lidí. Vzniklo také mnoho upravených verzí a parodií, například s přidanými světelnými a jinými efekty. Chlapec byl také parodován v seriálu South Park – epizoda byla vysílána v roce 2008.

Obr. 18. Případ "Star Wars kid"

Ghyslain Raza se po zjištění nečekaně nabyté popularity psychicky zhroutil a musel se podrobit dlouhodobé léčbě. Incident měl také soudní dohru, když chlapcova rodina zažalovala 4 jeho spolužáky o 250 000 kanadských dolarů. Případ skončil mimosoudním vyrovnáním.

2.5 Zneužití falešné identity

Zneužití falešné identity se někdy také označuje výrazem „Cybergrooming“. Jedná se o snahu pachatele skrýt se na sociální síti za někoho jiného, čehož docílí nejčastěji vytvořením profilu s falešnými osobními údaji. Nejčastější cílovou skupinou pachatelů jsou malé děti a mladiství. Jejich důvěřivosti zneužívají například k vylákání na schůzku a následnému zneužití, v širším úhlu pohledu lze také mluvit o možnosti jejich manipulace. Jedná se o jedno z nejvyšších bezpečnostních rizik, s jakým se lze na internetových sociálních sítích setkat, proto je třeba náležitě analyzovat veškerý průběh jeho zneužití od prvotní přípravy na kontakt s obětí až po její setkání s pachatelem. Této analýze se věnují následující kapitoly.

2.5.1 Příprava na kontakt a jeho realizace

Příprava na kontakt s obětí má několik fází:

- **Výběr sociální sítě** – útočník se ze všeho nejdříve seznámí s rozhraním sociální sítě. Vybírá si nejčastěji takovou síť, kde je potencionálně největší koncentrace obětí, především dětí a mladistvých. Často se může stát, že se útočník na zvolené sociální síti již zdržuje a vystupuje zde pod svou skutečnou identitou.
- **Tvorba falešné identity** – tvorba falešného profilu je základním předpokladem k úspěšnému kontaktu. Útočník si vymyslí osobní údaje, které nejlépe odpovídají věkové skupině jeho oběti. Ve většině případů je jeho věk přímo úměrný věku uživatelů, s nimiž chce navázat kontakt. Z toho vyplývá skutečnost, že za předpokladu úmyslu seznámit se s dětmi a mladistvými, se takřka nesetkáme s případy, kdy je deklarovaný věk útočníka menší než věk oběti. Důvodem pro toto číslo je skutečnost, že často vystupuje jako vyšší autorita v rámci například fiktivní firmy, což v konečném důsledku znamená větší důvěryhodnost.

  Rozlišujeme dva typy falešné identity:

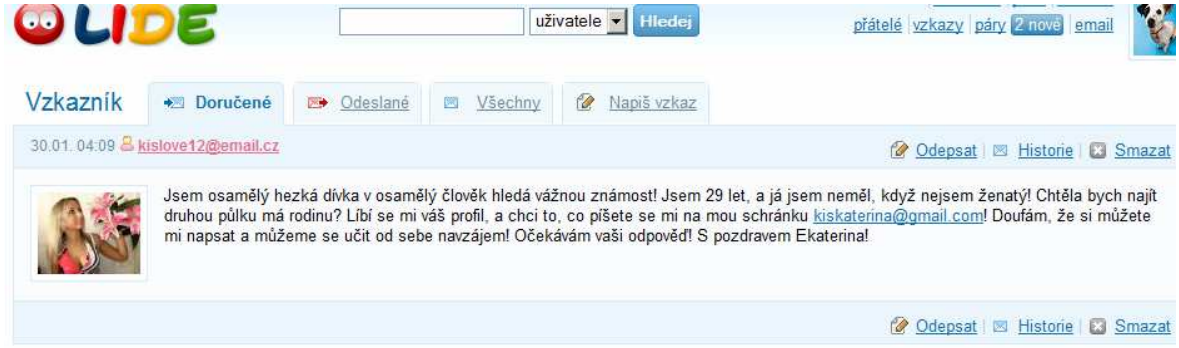
  - Statická – tento útočník má obvykle jen jeden profil a komunikuje s omezeným počtem obětí, což mu zajišťuje lepší přehled nad tím, co si s každým kdy napsal a riziko včasného odhalení je tedy menší.
  - Dynamická – pachatel často mění svou identitu i rozsah svého působení. Přizpůsobuje se aktuálním potřebám a mění často údaje ve svých profilech.

> Často komunikuje s více oběťmi, někdy i v rámci několika sociálních sítí. Důsledkem je složitější správa a kontrola informací, které o sobě kdy uvedl. Musí si vést záznamy o jednotlivých uživatelích a v případě chyby se vystavuje nebezpečí včasného odhalení. Tvorbu a správu dynamické identity bere jako výzvu.

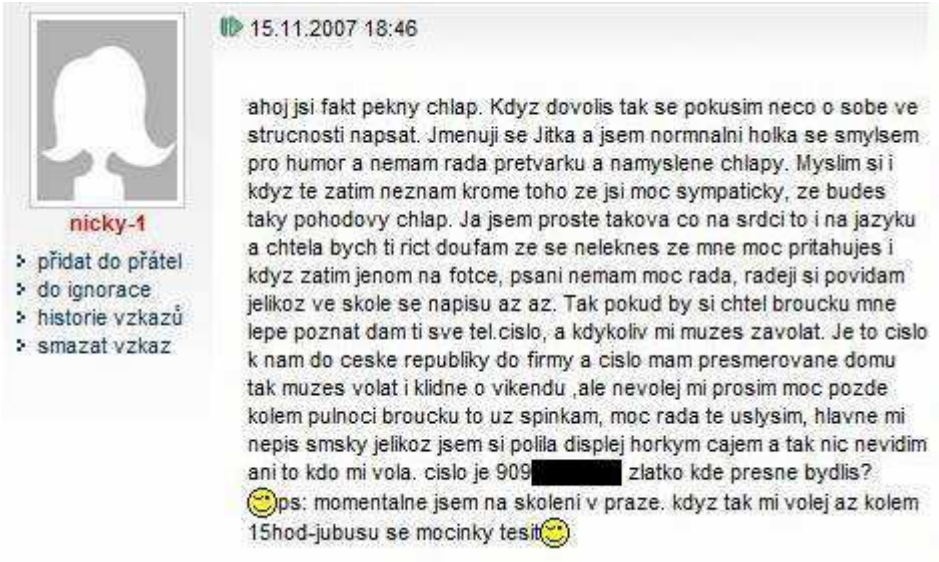
Vyšší autorita ve formě zástupce fiktivní společnosti bývá často používaným trikem, jak vylákat osobní údaje od uživatelů sociální sítě.

Samotný kontakt je nejdůležitější etapou seznámení. Rozlišujeme dva druhy kontaktu – přímý a nepřímý. Přímým kontaktem rozumíme kontaktování konkrétního vytipovaného uživatele. Nepřímým pak zaslání určité nabídky, nejčastěji ve formě soukromě zprávy na sociální síť, emailu nebo diskuzi či chat. Jedná se například o různé fiktivní soutěže, kdy je pro účast nezbytné zaslat své osobní údaje nebo se může jednat o různé nabídky k seznámení svázané falešnou identitou (nejčastěji profil mladé dívky).

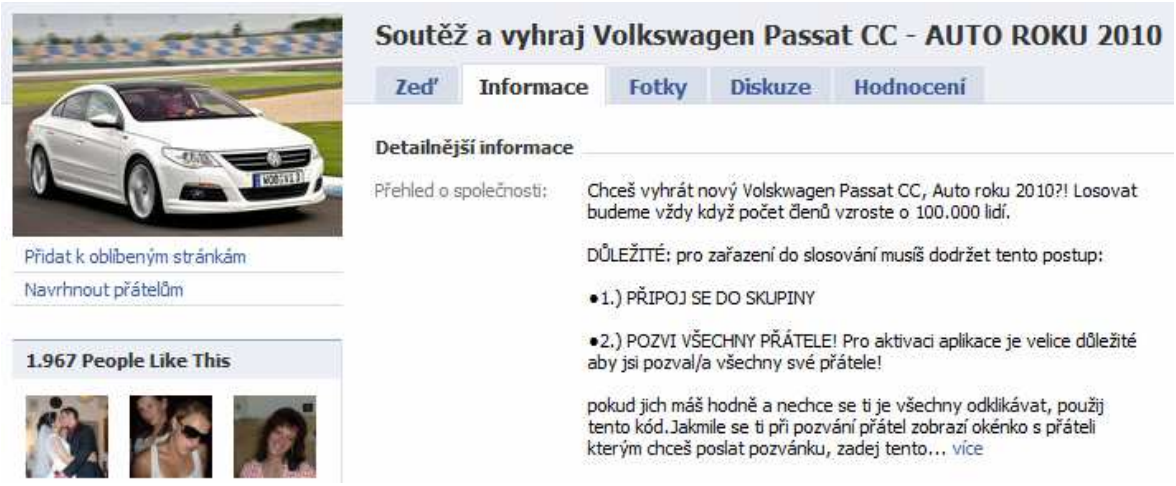
Níže jsou reálné případy nepřímého kontaktu z různých sociálních sítí.



Obr. 19. Inzerát svázaný s falešnou identitou



Obr. 20. Případ zneužití sociální sítě Líbímseti.cz



Obr. 21. Fiktivní soutěž určená ke sběru osobních dat uživatelů

2.5.2 Navazování a prohlubování vztahů

Navazování vztahů je další etapou manipulace s uživatelem. Charakteristickým znakem manipulátorů je tzv. schopnost zrcadla. Principem je kopírování chování a přizpůsobení se pocitům oběti. Ta pokud napíše, že má nějaký problém, útočník se okamžitě přizpůsobí a tento problém v podstatě přenese na sebe způsobem, že oběť pak nabude pocitu, že její virtuální přítel má stejná trápení a svěřuje se mu s dalšími podrobnostmi. Útočník zpravidla volí slova, ze kterých vyplyne, že má podobné problémy a že tedy plně chápe důsledky tohoto problému. Jeho přátelství je tak upevňováno a oběť se mu svěřuje s dalšími problémy a jako odpověď se jí vždy dostane pochopení. Tato iluze je obzvláště

nebezpečná, neboť pokud je překročena určitá mez, oběť již nemá v komunikaci zábrany a může svolit k osobnímu setkání. Není přitom kopírována pouze emoční stránka, ale také koníčky, názory, povaha, apod. Důsledky této fáze manipulace jsou již zřetelné v chování oběti a ta i po včasném odhalení změn jejím okolím si své počínaní bez výčitek obhájí.

Příklad komunikace s využitím metody zrcadla:

Johny_x >> Ahoj, jak se máš?

Jana16 >> Dobře, ale nudím se.

Johny_x >> Já se mám také v pohodě, ale v poslední době nemám co podniknout.

Jana16 >> To jsme dva.

Johny_x >> Můžeme se teda nudit spolu :D

Jana16 >> Tak dobře :P

Johny_x >> Kolik ti je vlastně let?

Jana16 >> 16.

Johny_x >> Mně je 18.

Johny_x >> A máš ráda nějaký sport?

Jana16 >> Rodiče mi koupili nové kolo tak s ním občas někam vyrazím.

Johny_x >> Ano? To je super! Já mám taky moc rád kolo! Odkud vlastně jsi?

iJana16 >> Jsem ze Zlína.

Johny_x >> To je ale náhoda! Já taky ☺Tak co kdybychom něco podnikli?

Další vlastností útočníků bývá snaha získat maximum informací o uživateli, jako je například škola, jména nejlepších kamarádů, zaměstnání rodičů, adresa bydliště, atd. Tato data mohou být dále využita k další přímé manipulaci. Další častou praxí bývá lehké směřování konverzace směrem k tématům o intimnostech a sexu, což souvisí s redukováním komunikačních bariér oběti.

2.5.3 Příprava na osobní setkání a jeho realizace

Agresor má nyní dostatek informací o uživateli a může tedy začít plánovat osobní setkání. I zde jsou používány metody pro cílenou manipulaci. Největším a často nepřekonatelným problémem útočníka je většinou věkový rozdíl mezi ním a obětí. I zde jsou však útočníci velmi vynalézaví a existují určité metody, jak tento věkový problém překonat. Agresor po několika týdnech komunikace oběti sdělí, že mu jeho otec zakázal přístup k internetu, ale že jeho starší bratr by mohl pokračovat v konverzaci jako prostředník. Tento člověk je samozřejmě opět fiktivní identita stejného útočníka. Oběť tento fakt často akceptuje a pokračuje v konverzaci. Následné setkání je opět otázkou manipulace a lží. Útočník domluví místo setkání, avšak následně se vymluví, že musí být například dlouho ve škole nebo na tréninku a že namísto sebe pošle svého otce nebo jiného rodinného příslušníka, který ji odveze na bezpečné místo, kde následně dojde ke konfrontaci a v nejhorším případě ke zneužití a někdy také k usmrcení oběti.

V případě odmítnutí uskutečnění schůzky ze strany oběti pak dochází k procesu vydírání, kdy agresor vyhrožuje zveřejněním choulostivých částí konverzace, případně fotografií a jiných dat, které mu oběť poskytla. Zveřejněním zde rozumíme například zaslání kompromitujícího materiálu řediteli školy, rodičům, kamarádům a podobně. Tento nátlak mnoho dětí psychicky neunese a raději svolí ke schůzce, než aby byly terčem výsměchu a urážek.

Následná schůzka, která byla útočníkovou motivací po celou dobu manipulace je vyvrcholením celého procesu. Na první schůzce obvykle nemusí dojít ke zneužití. Útočník si nejdříve ověří, zda se skutečně jedná o jeho vytipovanou oběť. Obvykle bývá doprovázena drobným darem a řádným vystupováním agresora, který tak jen upevní svou pozici „dokonalého přítele“. Následně záleží jen na jeho umu přesvědčování a manipulace a je jen otázkou času, kdy se pokusí o první intimní kontakt. Jen zřídka kdy má útočník výčitky svědomí, které mu zabrání dívku či chlapce zneužít, jelikož s jeho manipulací strávil mnoho času. Ojediněle z hlediska oběti může však paradoxně nastat platonická závislost na agresorovi, jejíž důsledky však již nejsou předmětem analýzy. Cílem práce je navrhnout postupy a konvence, jak se manipulaci bránit a jak tyto agresory dopadnout.

2.6 Pronásledování

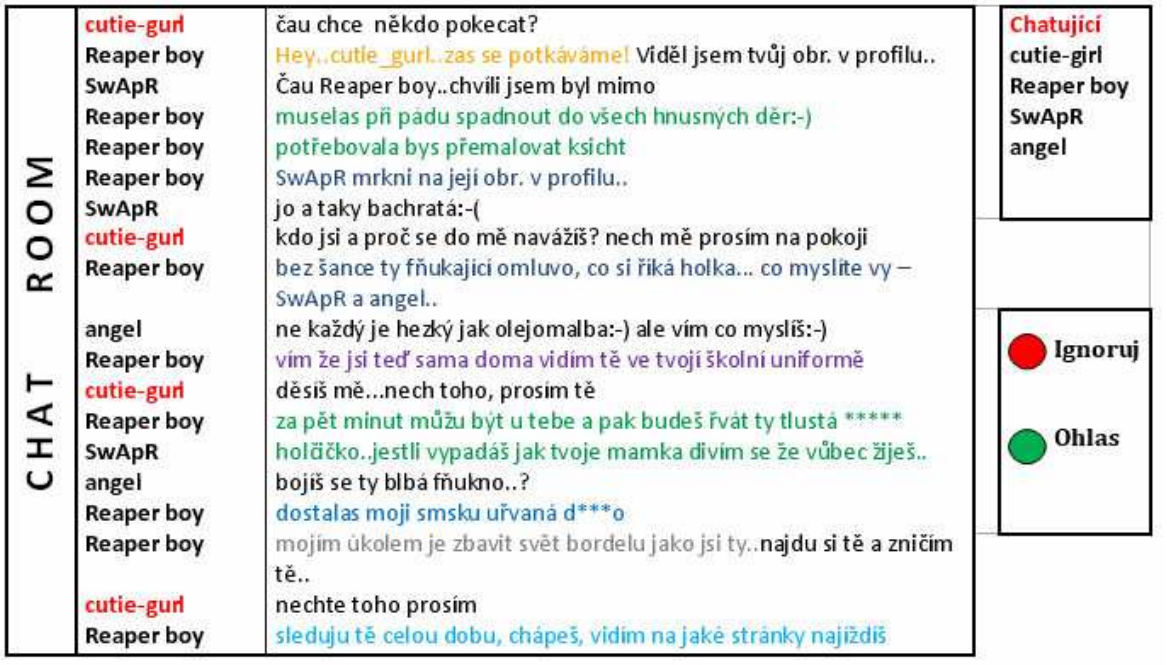
Pronásledování (Cyberstalking) je dalším problémem, který je specifický pro soudobé sociální sítě a můžeme jej definovat jako zneužívání komunikačních služeb k cílenému zasílání nevyžádaných zpráv, k pronásledování, obtěžování a zastrašování uživatelů. Pachatelé k páchání této trestné činnosti používají nejčastěji chaty, diskusní fóra, emaily a v neposlední řadě také sociální sítě, kde jsou všechny tyto funkce většinou zahrnuty. Pronásledování jako pojem příliš nevypovídá o povaze a motivaci útočníků. Je třeba jasně vymezit jejich chování a motivy, o což se pokusím dále v textu.

2.6.1 Výraz „stalker“

Stalker je anglický výraz pro lovce. V prostředí internetu jím rozumíme člověka, který úmyslně vyhledává osoby, kterým následně svým pácháním znepříjemňuje život a snižuje jeho kvalitu. Jeho osobní pohnutky způsobují vytrvalost v páchání trestné činnosti, jelikož chce negativně působit na co možná největší množství lidí. Jedná se většinou o jedince nespokojené se svým životem, jejichž smyslem života je působit zlovolně na své okolí, k čemuž využívá různých metod. Jedná se především o urážky jak v prostředí více uživatelů, tak formou soukromých zpráv či e-mailu. Rozesílá nevyžádané zprávy, které mohou obsahovat viry a jiný škodlivý obsah. Obětem může vyhrožovat a zastrašovat je, což zvláště u malých dětí může způsobit trauma a psychický otřes. Vyhrožování může zahrnovat například výhružky typu vyhledání oběti v reálném světě. Také se může snažit nabádat jiné uživatele k psychickému nátlaku na oběť. Zaměřuje se jak na jednotlivce, tak na skupiny. Pachatel ve většině případů svou oběť osobně nezná, avšak může se také jednat o formu pomsty za nějaký incident z reálného života.

Příklad konverzace, kdy skupina „stalkerů“ zastrašuje svou oběť, uvádí následující obrázek [4] obsahující výňatek z chatu:

[4] Obrázek je přejatý z webu e-bezpeci.cz, který se zaměřuje na informování veřejnosti o bezpečnostních nástrahách internetu. Konkrétně z adresy http://cms.e-bezpeci.cz/content/view/44/38/lang,czech/



Obr. 22. Příklad pronásledování

2.6.2 Motivace pachatelů

Motivace pachatelů mívá mnohdy stejné kořeny. Spočívá v pocitu moci a nadvlády nad oběťmi, který dává útočníkovi pocit síly. Může se také jednat o nácvik metod pro manipulaci s různými uživateli, které jsou dále zdokonalovány a následně použity k jinému, cílenějšímu útoku. Agresoři často operují ve skupinách a jednají koordinovaně. Často si za svůj cíl volí slabé jedince, kteří mohou na urážky reagovat hůře, než jiní lidé. Motivem pachatelů téměř nikdy nebývají peníze ani majetek.

2.6.3 Legislativa

Narozdíl od většiny jiných západních zemí neměla Česká Republika ve svém trestním řádu zakotven příslušný zákon zajišťující postih pachatelů za výše uvedené činy. Až 1.1.2010 došlo k zavedení postihu pronásledování (stalkingu), na které je od té doby nahlíženo jako na trestný čin.

2.7 Osobní údaje a jejich zneužití

2.7.1 Definice a vymezení

Zneužití osobních údajů je další z řady bezpečnostních rizik, kterým se uživatel na sociální síti vystavuje, pokud je zveřejní. Osobní údaj je dle definice § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů „*jakákoliv informace týkající se určené nebo určitelné fyzické osoby, k níž se osobní údaje vztahují. Tato se považuje za určenou nebo určitelnou, jestliže lze fyzickou osobu přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro její fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu*“.

Dle definice lze za osobní údaje označit například tyto:

- Celé jméno a příjmení
- Fakturační adresa
- Rodné číslo
- E-mailovou adresu obsahující jméno a příjmení – například petr_novak@seznam.cz
- Číslo sociálního zabezpečení, číslo pasu, atd.

Dále existují citlivé osobní údaje, dle kterých lze o konkrétním člověku zjistit informace týkající se jeho zdravotního stavu, sexuálních preferencí, náboženského a politického přesvědčení či osobních názorů.

2.7.2 Metody vylákání a zneužití osobních údajů

Analýza by se měla zabývat i metodami vylákání a případnými dopady zneužití osobních údajů na změnu kvality života. Mnoho organizací používá pro identifikaci klientů jejich osobní údaje, například pojišťovny pro komunikaci s klienty vyžadují většinou rodné číslo. Teoreticky tak na základě jeho znalosti spolu s přehledem o dalších údajích o uživateli se může útočník identifikovat na telefonní zákaznické lince jako oběť. Dle různých osobních údajů lze dále dohledat více informací o daném člověku.

Existují různé metody pro vylákání osobních dat různého charakteru včetně běžně neuváděných údajů, jako například adresa, zaměstnavatel, zdravotní stav či stav majetku. Často to bývá od samotné oběti či jejich známých.

Přímý přístup

„Útočník bez okolků přímo požádá oběť (například recepční) o její uživatelské jméno a heslo. I tato metoda může mít někdy nárok na úspěch.“ [12]

Důležitý uživatel

„Útočník předstírá, že je někým z vedení firmy, má problémy, které velice rychle potřebuje vyřešit a požádá o informace typu: typ používaného software pro vzdálený přístup, jeho konfiguraci, telefonní čísla k vytáčení, další informace nutné k přihlášení se k serveru. Pracovník technické podpory samozřejmě "nadřízenému" rád pomůže (nerad by měl konflikty a nerad by přišel o práci).“ [12]

Bezmocný uživatel

„Útočník si vybere identitu například nového zaměstnance (nebo zaměstnance nepříliš zručného v ovládání počítače), který má potíže s prvním přihlášením do firemní sítě (popřípadě zapomněl heslo a nutně potřebuje pracovat na svém projektu). Skutečný zaměstnanec-oběť se snaží dotyčnému pomoci (pracujeme přeci v jedné firmě, v jednom týmu, tak proč nepomoci), například tím, že dočasně poskytne útočníkovi své uživatelské jméno a heslo, v případě administrátora pak tím, že například vygeneruje pro daný účet nové heslo.“ [12]

Pracovník technické podpory

„Útočník předstírá, že patří do firemního oddělení informatiky. Tímto způsobem lze získat zaručeně pravdivé informace od běžných uživatelů. Typicky může jít o zaslání e-mailu, který se tváří, že je od administrátora a požaduje s jakýmkoli odůvodněním znovupotvrzení loginu a hesla. Řadoví zaměstnanci, kteří nejsou školeni, samozřejmě nemají ani ponětí o tom, že hlavička Odesílatel vůbec nemusí obsahovat pravdivé informace.“ [12]

Obrácená sociotechnika

„Situace se obrátí. Útočník obvykle zaranžuje události tak, aby se na něj s prosbou o pomoc obrátila samotná oběť.“ [12]

2.8 Závislost na sociální síti

Další nebezpečí internetových sociálních sítí spočívá v možnosti vzniku závislosti a odcizení se od reality a od společnosti. Sociální síť je jako komunikační nástroj využíván v soukromém i veřejném sektoru. Ve veřejném sektoru slouží především jako jedno z médií pro komunikaci se zákazníky a prezentaci firmy. V soukromém pak primárně pro setkávání s přáteli. Je známo, že velké sociální sítě s množstvím funkcí a podpůrných aplikací udrží člověka u obrazovek mnohem déle, než je nezbytně nutné. Zvláště jsou to:

- „zeď“ nebo jiný souhrn aktuálních událostí a poslední činnosti přátel a jejich „statusů“
- fotogalerie a hodnocení jednotlivých fotografií s možností komentářů
- hry pro jednoho i více hráčů
- chat a další funkce pro přímou komunikaci mezi dvěma a více lidmi
- možnost aktualizace vlastních stavů

Tyto a další funkce udržují aktivitu uživatele na sociální síti a působí také jako stimulační prvek, aby se uživatel měl důvod vracet. Lidé sociálním sítím věnují svůj volný čas, avšak mnohdy bývá návyk na sociální síť tak velký, že jsou zanedbávány jiné ‚důležitější aktivity.

Dobrý náhled na problematiku návyku uživatelů na sociální sítě podává průzkum internetového obchodu Retrevo[5], který si nyní představíme. Vyplývají z něj mnohdy zajímavé až šokující závěry, které vypovídají o možnosti vytvoření závislosti.

[5] Průzkum lze nalézt na adrese http://www.retrevo.com/content/blog/2010/03/social-media-new-addiction

2.8.1 Průzkum závislosti uživatelů na sociálních sítích

Uživatelé odpovídali na sadu otázek týkajících se jejich aktivity na konkrétních sociálních sítích – Facebook a Twitter. Uživatelé kromě odpovědí vyplnili také svůj věk a platformu, odkud k sociální síti přistupují. Otázky byly následující:

- Kontrolujte a/nebo aktualizujete svůj profil na Facebooku nebo Twitteru poté, co jdete spát?
- Je první věcí, kterou ráno uděláte, návštěva profilu na Facebooku nebo Twitteru?
- Jak dlouho vydržíte nekontrolovat svůj profil na Facebooku?
- Je možné vás vyrušit elektronickou zprávou při uvedených činnostech?

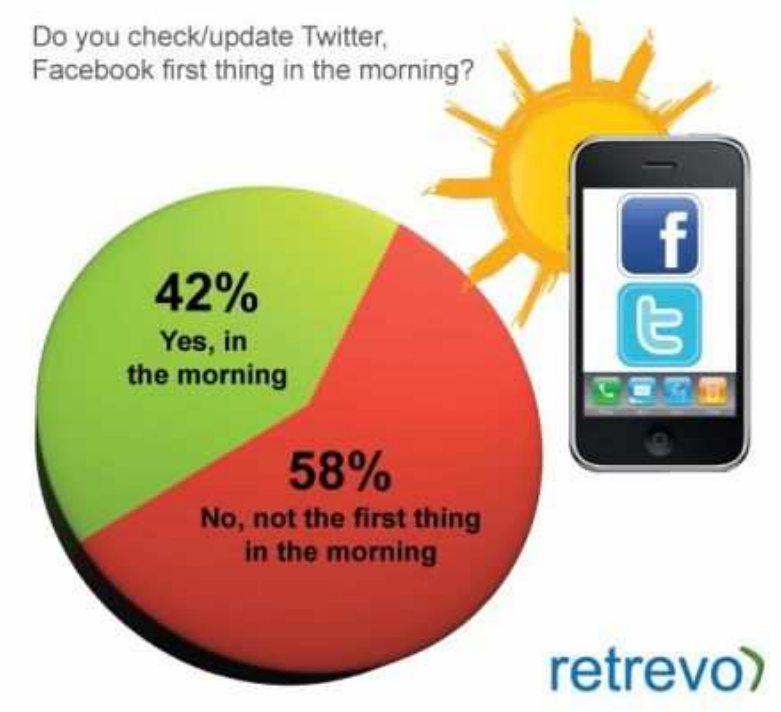
Výsledky první otázky jsou následující:

Obr. 23. Výsledky otázky č.1

Obr. 24. Výsledky otázky č.1

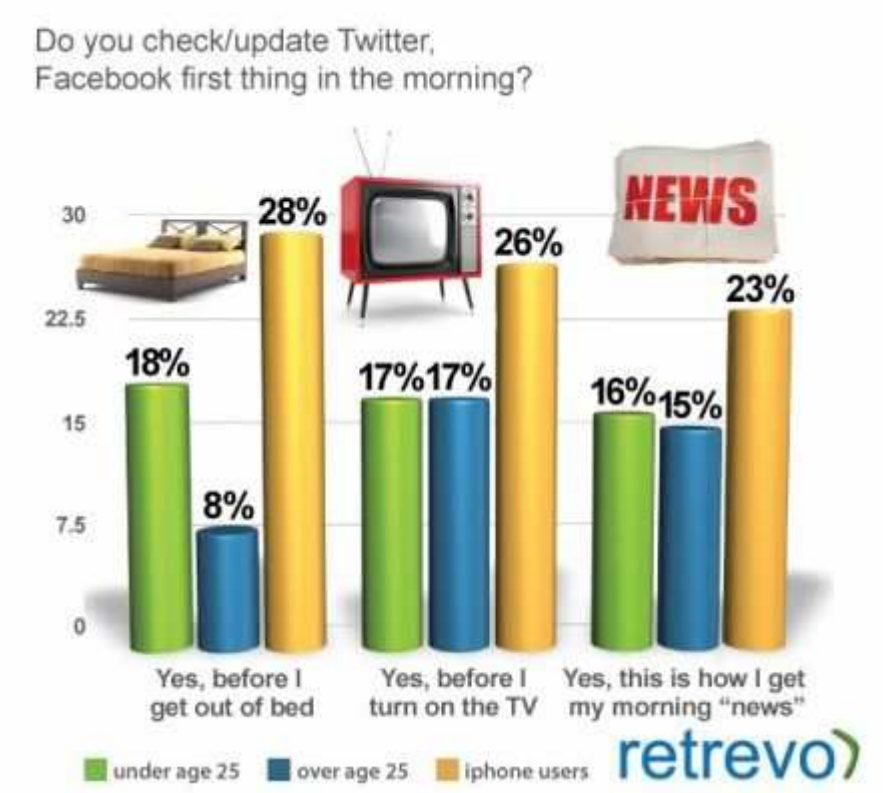
Na první otázku, zda uživatelé kontrolují svůj profil i v době, kdy by měli spát, odpověděla téměř polovina respondentů kladně. 48% dotázaných skutečně buď v noci nebo ihned po probuzení kontroluje svůj profil. Z dalšího grafu je vidět, že velká část ze zmíněných 48% uživatelů (konkrétně 32% uživatelů mladších 25 let, 21% starších než 25 let) kontroluje svůj profil ráno ihned po probuzení. Dalších 46%, respektive 31% kontroluje svůj profil alespoň jednou za noc. Toto jsou příliš velká čísla a je z nich vidět, že lidé mladší 25 let jsou obecně do sociálních sítí více zapálení. Vzhledem k vyšší absenci zaměstnání a tedy více volného času je tento závěr logický, avšak vzhledem k povinné školní docházce alarmující.

Druhá otázka, zda první ranní činností je kontrola sociální sítě, nedopadla o nic lépe.



Obr. 25. Výsledky otázky č.2

42% respondentů ráno kontroluje sociální síť, což je možná lepší, než v noci. I tak jsou však dle mého názoru důležitější věci na práci a nejen že uživatelé zanedbávají sami sebe, ale ztrácí čas kontrolou sociální sítě, což v konečném důsledku, když už mají potřebu na sociální síti být, mohou udělat například až ve vozidle městské hromadné dopravy. Uživatelé, kteří odpověděli na tuto otázku kladně, jsou shrnuti v dalším grafu.



Obr. 26. Výsledky otázky č.2

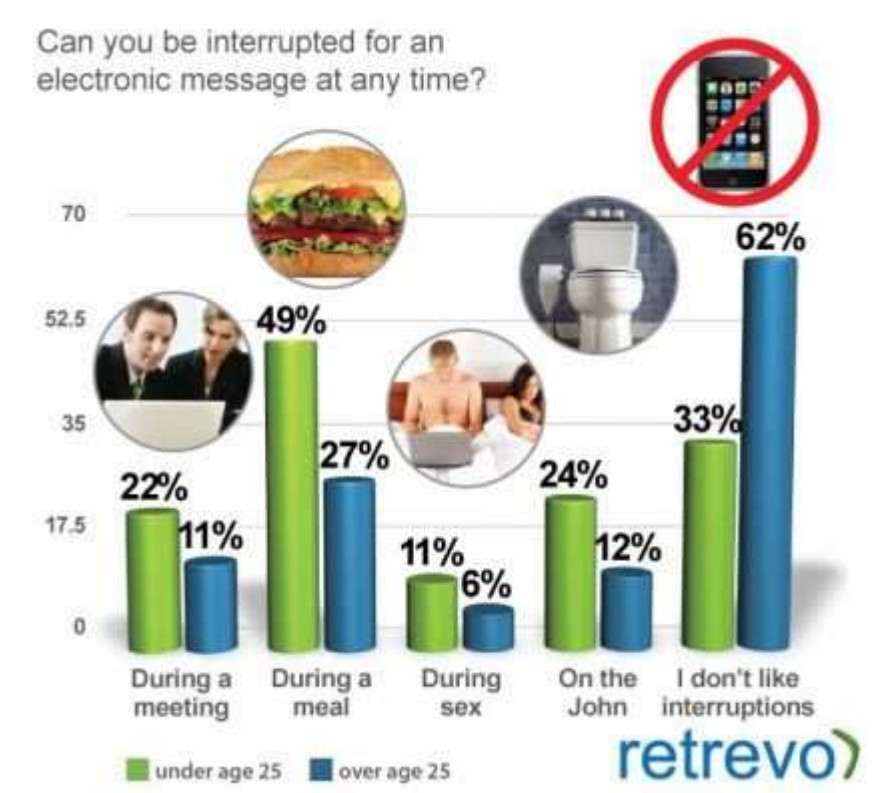
Z grafu je možno vysledovat, že osoby mladší 25 let kontrolují svůj profil po ránu velmi často ještě v posteli. Nejvíce mne na tomto závěru zaráží fakt, že tito uživatelé zcela jistě kontrolují sociální síť také před spaním. Opravdu je nezbytně nutné navštěvovat sociální síť, abychom se dozvěděli, co se událo přes noc, kdy většina populace spí?

Další otázka zachází ještě dál a týká se toho, jak dlouho uživatelé vydrží bez kontroly sociální sítě. Výsledky můžeme již odvodit z předchozích dvou otázek.

Obr. 27. Výsledky otázky č.3

Z grafu vyplývá, že 60% osob mladších než 25 let nevydrží bez sociální sítě více než jeden den. Jedna pětina dokonce ani několik hodin. Výsledek kopíruje výsledky minulých otázek, jelikož dle mého názoru, pokud uživatel navštíví sociální síť ráno, navštíví ji tentýž den většinou ještě minimálně jednou.

Poslední otázka se týká provázanosti sociálních sítí s každodenním životem. Nabízí pohled, jak moc se jimi lidé nechávají ovlivňovat při svých každodenních činnostech. Modelovou situací pro vysvětlení podstaty problému může být například rodinný oběd, kdy se tradičně sejde celá rodina u jednoho stolu. Již na základní škole je dětem vysvětlováno, že odcházet od stolu bez zjevného neodkladného důvodu je neslušné v jakékoli společnosti. To však již pomalu přestává platit, což lze ilustrovat například výpovědí několika dotázaných rodin s dospívajícími dětmi, kdy většina z nich po prvním chodu odběhne k počítači, pravděpodobně zkontrolovat svůj profil nebo aktualizovat svůj stav na sociální síti. Toto jen dokazuje rostoucí závislost na sociální síti. Jak ukazuje následující graf, tento trend je opět devizou osob mladších 25 let.



Obr. 28. Výsledky otázky č.4

Výsledky jsou opět alarmující. Z grafu je vidět, že relativně velkému procentu osob mladších než 25 let nevadí vyrušení od dotazovaných aktivit, zatímco s rostoucím věkem se naštěstí provázanost se sociální sítí zmenšuje spolu s uvědoměním si, že jsou pravděpodobně důležitější aktivity, než neustálá kontrola sociálních sítí. Osoby ve věku nad 25 let se nechají vyrušit zprávou ze sociální sítě ve všech případech téměř o 50% méně, než uživatelé mladší. Vliv sociálních sítí má však zatím stoupající tendenci a bude pravděpodobně ještě větší.

3 NÁVRH KONVENCÍ MINIMALIZUJÍCÍ BEZPEČNOSTNÍ RIZIKA

Nejzranitelnějším článkem každého systému je i přes veškerou snahu vždy uživatel, který tento systém používá. Nejinak je tomu i u sociálních sítí, které jsou silným nástrojem usnadňujícím komunikaci a sdílení dat. Jejich používání nese řadu výhod, avšak vzhledem k neinformovanosti veřejnosti, jejíž velká část je počítačově negramotná, stále častěji dochází ke zneužití sociální sítě vůči jejím uživatelům. Analyzovaná bezpečnostní rizika vždy představují potencionální nebezpečí pro uživatele jakékoliv věkové kategorie. Nejvíce jsou však postihovány děti a mladiství, kteří využívají internet ve stále větším měřítku. Bohužel, při výskytu jakéhokoliv problému bývá již většinou pozdě hledat jeho příčinu. Rčení, které říká, že chybami se člověk učí, by v tomto případě nemělo platit. Jedna chyba může mít fatální následky jak na počítačovou stanici, tak na člověka, který s ní operuje, přičemž následky na člověku jsou většinou mnohem těžší a v mnoha případech nevratné. Je proto třeba především důsledně dbát na **prevenci**. Přestože existují různé iniciativy pro podporu informovanosti veřejnosti, především dětí, stále se jedná jen o pokrytí malého procenta populace. Následující kapitoly uvažují návrhy, které by v konečném důsledku významnou měrou přispěly ke zvýšení bezpečnosti pohybu nejen na sociálních sítích.

3.1 Prevence na straně uživatele

Prevencí na straně uživatele rozumíme všechny aspekty, které je možné ovlivnit, aniž by zároveň byla nutná změna koncepce a implementace funkcí sociální sítě.

3.1.1 Shrnutí výsledků analýzy

Analyzoval jsem potencionální bezpečnostní rizika. Každé je svým způsobem specifické a vyžaduje různé přístupy, jak se mu bránit, či v lepším případě úplně vyhnout. Z výsledků analýzy lze vyvodit, že nejslabším článkem každého systému je v dnešní době vždy uživatel, který útočníkovi může přímo či nepřímo usnadňovat práci. S neustálým vývojem a nepříliš velkou informovaností cílových uživatelů pak zneužití těchto rizik neustále roste. V této kapitole navrhuji konvence, které při použití minimalizují možnost zneužití či případného dopadu na uživatele. V současné době však neexistuje prostředek, jak efektivně

uživatele sociálních sítí informovat. Můj další návrh se proto týká integrace výuky o počítačové kriminalitě do stávajícího systému školství.

3.1.2 Pravidla pro pohyb na sociálních sítích – návrh konvencí

Uvádějte o sobě jen nezbytně nutné informace

Některé sociální sítě využívají různé techniky pro získání co možná největšího množství pravdivých informací. Tato praxe je zvláště patrná u sítí provozujících vlastní systém cílených reklam, kdy jsou tato data nezbytná pro cílení inzerce. Firmy provozující komunitní weby shromažďují obrovské množství citlivých osobních údajů, které alespoň z části určují hodnotu dané firmy. Čím více dat provozovatel spravuje, tím větší motivaci má útočník k jejich získání. Vždy také existuje možnost odkupu těchto dat jinými společnosti nebo příkaz na jejich vydání od správního orgánu.

Používejte jen prověřený software spolu s nainstalovaným antivirovým programem

Neustále vznikají nové hrozby v podobě virů a jiných škodlivých kódů, které mohou poškodit váš počítač či z něj ukrást citlivá osobní data, jako jsou hesla k internetovému bankovnictví. Tento speciální software se šíří nejenom přes e-mail, ale stále častěji využívá platforem sociálních sítí. Je potřeba používat prověřený webový prohlížeč se správným nastavením úrovně zabezpečení spolu s nainstalovaným antivirovým programem s nejnovějšími aktualizacemi. Tímto opatřením se sníží riziko napadení počítače škodlivým softwarem na zanedbatelnou úroveň.

Nepřidávejte si mezi své přátele lidi, které neznáte. Před schválením žádosti o přátelství si ověřte totožnost žadatele například kontrolní otázkou či mobilním telefonem.

Vytvoření profilu s falešnými údaji je velmi snadné a bohužel není šance zjistit, zda se za ním skrývá deklarovaný vlastník nebo podvodník. Proto před každým schválením žádosti o přátelství položte kontrolní otázku, na kterou by měla znát odpověď jen vám známá osoba. Nejúčinnější prevencí pak je schvalování žádostí v přítomnosti obou stran. Pokud máte podezření, že se jedná o falešný profil, kontaktujte odpovědnou osobu.

Pozorně kontrolujte veškeré žádosti aplikací sociální sítě o přístup k vašim osobním údajům.

Obr. 29. Příklad žádosti o povolení přístupu k osobním údajům

Příklad na tomto obrázku ukazuje jednu z aplikací sociální sítě Facebook, která žádá o povolení k přístupu k osobním údajům. Svolením dáváte potencionálnímu útočníkovi snadný přístup k vašim datům, mezi něž patří i fotografie, jméno a příjmení, seznam přátel a další informace. Tato data mohou být následně prodána a využita k marketingovým účelům, jako je cílená inzerce.

Nikdy neudávejte svoji aktuální, ani budoucí geografickou polohu, pokud je vám známá.

Je třeba si uvědomit, že vyzrazením své aktuální polohy dáváte potencionálnímu útočníkovi cennou informaci, kterou může využít například k vykradení domu či bytu.

Na sociální síť (a obecně na internet) přistupujte vždy jen ze svého počítače.

Nikdy nevyužívejte cizí počítače, o kterých si nejste zcela jisti, že zde není nainstalován speciální software určený pro sledování uživatelů. Jedná se například o ukládání posloupnosti stisku jednotlivých kláves, kdy je možné vysledovat zadané přihlašovací údaje (jméno a heslo) a následně je zneužít. Setkáváme se také s monitorováním síťového provozu, ze kterého lze kromě navštívených stránek při nezabezpečeném připojení získat také citlivá data.

Nepoužívejte sociální sítě jako prostředek k seznámení s jinými lidmi.

Po přečtení analýzy jistě dojdete k závěru, že v prostředí sociální sítě není možné mít důvěru k neznámým lidem, jelikož vždy existuje šance, že se na druhé straně skrývá agresor.

Používejte pouze bezpečná hesla s délkou 8 a více znaků při současném použití malých i velkých písmen, čísel a dalších symbolů. Nikdy nepoužívejte stejné heslo na všech stránkách, kde se registrujete. Používejte náhodnou posloupnost znaků.

Heslo měňte minimálně jednou za 3 měsíce. Existují různé generátory bezpečných hesel[6], které můžete použít namísto vymýšlení vlastního. Heslo si nikdy nezapisujte. Kromě vymýšlení náhodných posloupností znaků existuje také několik technik pro výběr hesla. Jedna z nich je výběr jakékoliv věty obsahující alespoň 8 slov. Počáteční písmeno každého slova bude tvořit heslo. Například:

„Můj oblíbený sportovní tým je od 6 let Sparta Praha“. Výsledné heslo je „Mostjo6lSP“. Můžeme konstatovat, že zvolené heslo, respektive věta se bude pravděpodobně dobře pamatovat jejímu autorovi, avšak potencionální útočník má k jeho rozluštění jen malou šanci.

[6] Příklad generátoru využívající algoritmus generování bezpečného hesla: http://www.thebitmill.com/tools/password.html

Používejte více než jednu e-mailovou schránku. Jednu pro soukromé účely a další pro účely registrace na sociálních sítí.

Toto opatření má za účel zamezit nevyžádané elektronické poště. Vždy existuje možnost úniku citlivých údajů z databáze provozovatele sociálních sítí, e-mailové adresy nevyjímaje. Ty mohou být navíc různě kategorizovány, například dle věku, rasy, zájmů, národnosti, atd.

Nikdy neodpovídejte na žádné, i sebevíce lákavé nabídky (soutěže), které jsou publikovány na neověřených a podezřelých stránkách.

V mnoha případech se jedná o produkt organizované skupiny útočníků, kteří tak mají zjednodušený přístup k vašim osobním údajům.

Každé podezření na porušení pravidel sociální sítě, dobrých mravů, obtěžování, urážky či vyhrožování nahlaste zodpovědné osobě.

Zodpovědnou osobou zde rozumíme například administrátora, který má přístup k dalším údajům pachatele (IP adresa, přehled o jeho chování) a má pravomoc zakázat agresorovi další přístup do sociální sítě a pří podezření na porušení zákona kontaktovat policii.

Zabezpečte si svůj profil nastavením vyšší úrovně soukromí.

Každá sociální síť by měla umožňovat nastavit komu co zobrazovat. Například Google Plus umožňuje nastavit kruhy uživatelů, kdy každému z nich je možné nastavit přístupové atributy.

Ignorujte veškeré žádosti o přidání do seznamu přátel, pokud se jedná o cizince a lidi, o kterých jste nikdy neslyšeli.

Na sociálních sítích se stejně jako v téměř každém veřejném systému pohybují fiktivní uživatelé vytvoření za účelem shromažďování osobních údajů od lidí, kteří akceptují žádost o přátelství.

Sociální síť nejlépe vůbec nepoužívejte.

Toto řešení zaručuje zánik všech bezpečnostních rizik, které s sebou sociální sítě přinášejí.

3.1.3 Metody pro dopadení agresorů

Stejně jako útočníci zneužívají chyb a slabosti uživatelů sociální sítě, můj další návrh se týká použít jejich vlastní zbraň proti nim samotným. Jedná se především o schopnost manipulace. Již v mnoha západních zemích se používá metoda vyslání agentů namísto skutečných obětí na místo setkání, přičemž v záloze bývají i ozbrojené složky připravené kdykoliv zasáhnout. Technika spočívá v rozpoznání podezřelého chování útočníka, který se všemi možnými způsoby snaží se svou obětí sejít. Toto rozpoznání je často i největší úskalí metody, jelikož většina dětí se bojí svěřit rodičům či jiné autoritě se svým problémem a jedná na vlastní pěst. Je však jasné, že je to pouze iluze způsobená negativními emocemi, jelikož dítě si většinou neuvědomí, že útočník mu nemůže přes virtuální prostředí ublížit. Přesto raději volí osobní setkání, kde se vystavuje mnohonásobně většímu riziku. Po domluvení místa setkání je vyslán namísto oběti vyškolený agent, který může snáze identifikovat útočníka.

3.1.4 Integrace do systému školství

Systém školství dle mého názoru neposkytuje řádnou přípravu dětí na nástrahy, které je mohou na internetu potkat. Jedná se přitom o nemalé nebezpečí, které může skončit kromě majetkových ztrát také psychickým otřesem nebo dokonce smrtí oběti.

Sociální sítě jsou stále více cíleny právě na děti, které s nimi vyrůstají již od útlého věku. Vzhledem k tomu by mělo existovat podvědomí o potencionálním nebezpečí internetových sociálních sítí. Právě z toho důvodu by mělo být do výuky zahrnuto seznámení s těmito riziky.

Integrace by měla zahrnovat včlenění do školního řádu s jasně definovanými přestupky a jejich postihy. Především by se měly aktualizovat předpisy týkající se počítačových učeben s možností připojení k internetu. Je potřeba kontrolovat, jaké stránky děti navštěvují a v nejlepším případě zakázat přístup na rizikové weby včetně sociálních sítí. Učitel by měl být obeznámen s veškerými bezpečnostními riziky a informovat o nich také rodiče žáků.

Můj další návrh se týká zavedení pravidelně se opakujícího anonymního průzkumu mezi žáky, jehož úkolem bude zjistit jejich zkušenosti s patologickými jevy na sociálních sítích. Tento průzkum by zároveň sloužil jako indikátor úspěšnosti prevence jednotlivých škol.

3.2 Prevence na straně serveru

3.2.1 Shrnutí výsledků analýzy

Z analýzy vyplývá, že sociální sítě jsou koncipovány především jako monetární prostředek a soukromí a ochranu svých uživatelů staví na vedlejší kolej. Bohužel, společnosti, které tyto sítě provozují, investují mnohem více prostředků do zvýšení své pozice na trhu na úkor vývoje nových bezpečnostních opatření. Jako příklad můžeme uvést například naprostou absenci zabezpečeného přenosu dat přes protokol SSL[7]. Dalším velkým problémem je nepřímé navádění uživatelů některých sociálních sítí ke zveřejnění co největšího objemu pravdivých osobních údajů, které jsou následně použity k cílení inzerce, která je hlavním zdrojem příjmu. Je jasné, že ideální model bezpečné sociální sítě, který je prezentován v další kapitole, není již z principu možný, avšak dle mého názoru není možné bez aplikace těchto pravidel mluvit o bezpečné sociální síti.

3.2.2 Ideální model bezpečné internetové sociální sítě

Ideální sociální síť by měla obsahovat následující prvky zabezpečení a mít následující vlastnosti:

- komunikace probíhající přes protokol SSL
- regulace sběru osobních údajů, zákaz využívání k marketingovým účelům
- možnost rychlého nahlášení nevhodného a podezřelého chování
- soukromí standardně ihned po registraci uživatele nastaveno na maximální zabezpečení dat
- správa oprávnění, kdo, kdy a z jakého důvodu má přístup k určitému obsahu uživatele
- rodičovská kontrola, omezení funkcí a maximální zabezpečení pro děti a mladistvé do 18 let

[7] Kryptografický protokol pro zabezpečený přenos dat mezi dvěma počítači.

- odpovědnost provozovatele sociální sítě za škody způsobené útočníky prostřednictvím jejich platformy
- zobrazení upozornění na možná bezpečnostní rizika před registrací, stejně jako můžeme vidět například na krabičkách cigaret.
- striktní interní politika
- dobře napsaný software, u nějž je doba nalezení a případné zneužití bezpečnostní chyby nákladnější než odcizená data.

Na druhou stranu, není možné pravděpodobně aplikovat všechny bezpečnostní funkce (anonymita, pseudonymita, nespojitelnost, nepozorovatelnost), jelikož tato pravidla nejsou aplikovatelná v reálném světě. V opačném případě by nikdo nikoho neznal. Posláním sociálních sítí je naopak tvorba vazeb mezi uživateli, kteří k sobě mají určitý vztah a použití těchto funkcí je irelevantní.

3.2.3 Bezpečnost zdrojového kódu, softwarová architektura

Každá sociální síť je vyvíjena lidmi, kteří v určité míře dělají chyby ve zdrojovém kódu. Zneužití těchto bezpečnostních chyb je pak jen otázkou času a šikovnosti útočníka či skupiny útočníků. Již několikrát v historii sociálních sítí se stalo, že byla taková chyba zneužita a je pravděpodobné, že budou zneužity i v budoucnu. Potencionálně jsou tak ohroženi všichni uživatelé jakékoliv aplikace v prostředí internetu. Špatně promyšlená softwarová architektura, laxnost při administraci a chyby ve zdrojovém kódu mohou zapříčinit obrovské úniky dat. Jako příklad lze uvést sociální síť Facebook, prostřednictvím jejichž agendy „Základní informace o uživateli“ bylo možné zjistit informace o jakémkoli uživateli bez ohledu na to, jakou měl nastavenu míru zabezpečení soukromí. Tato bezpečnostní chyba byla přístupná i přes upozorňování od samotných uživatelů několik dní, než ji provozovatel aplikace opravil. Bezpečnostní chyba se nevyhnula ani sociálním sítím Twitter a MySpace. U první jmenované měl útočník možnost měnit aktuální status jakéhokoliv uživatele. Druhá jmenovaná síť umožňovala na jakýkoliv profil vložit speciální kód v jazyce Javascript, který mohl přesměrovat přistupující uživatele na podvodné stránky.

Nejsou to však jen tyto tři případy. Každý měsíc jsou zaznamenávány v různé míře nové bezpečnostní hrozby, které mohou přímo ohrožovat uživatele sociální sítě. Vzhledem ke

konkurenčnímu boji je každá úspěšná a inovativní funkce nasazená jedním systémem téměř okamžitě implementována i do konkurenčních aplikací. Absence důkladného testování v celém průběhu programování pak může zapříčinit vznik bezpečnostních chyb ve zdrojovém kódu.

Můj další návrh se tedy týká samotné metodiky programování a implementace nových funkcí s ohledem na bezpečnost. Jedná se o posloupnost doporučení, jejichž dodržování by mělo zamezit většině neúmyslných chyb, které mohou nastat při programovém návrhu:

- Snaha programovat software typu „Secure by design“ – bezpečný díky návrhu a použití principu hloubkové ochrany.

Tento přístup má za úkol najít takový návrhový vzor, aby jeho znalost neohrozila bezpečnost aplikace. Znalostí návrhového vzoru zde rozumíme především schopnost odhadnout běh programu, tedy procedur, které při svém běhu program provede. Program by měl být schopen pracovat s minimem oprávnění, přičemž by mělo být zamezeno použití vyšší vrstvy vrstvou nižší, což i v případě chyby zamezí ohrožení funkce celého systému. Je potřeba ošetřit všechny nedůvěryhodné vstupy a předpovídat veškeré chování potencionálních útočníků. Každá funkce by měla být chráněna bezpečnostními mechanismy pracujícími v různých vrstvách. Selhání jednoho mechanismu by mělo být ošetřeno funkcí na další úrovni.

- Snaha o maximální bezpečnost ve všech fázích návrhu

Fáze návrhu software začíná na obchodní úrovni, kdy jsou navrženy funkce a vlastnosti systému. Již v této fázi by mělo být myšleno na striktní bezpečnostní politiku.

- Důkladná verifikace řešení

Úkolem verifikace je ověřit správnost návrhu ve všech fázích řešení.

3.3 Projekty pro ochranu dětí a mládeže

Vzhledem k prohlubujícímu se problému s bezpečností na internetu vznikly a neustále vznikají různé iniciativy jak v režii státu, tak soukromých institucí. Představení následujících organizací cituji z příslušných oficiálních prezentací.

3.3.1 Projekt e-bezpečí.cz

„Projekt E-Bezpečí je celorepublikový projekt zaměřený na prevenci, vzdělávání, výzkum, intervenci a osvětu spojenou rizikovým chováním na internetu a souvisejícími fenomény. Projekt je realizován Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého ve spolupráci s dalšími organizacemi.“ [16]

„Projekt se zaměřuje na nebezpečné internetové fenomény, které ohrožují jak děti, tak i dospělé uživatele internetu.“ [16]

„Projekt E-Bezpečí se specializuje zejména na:

- *kyberšikanu a sexting (různé formy vydírání, vyhrožování, poškozování obětí s pomocí informačních a komunikačních technologií),*
- *kybergrooming (komunikace s neznámými uživateli internetu vedoucí k osobní schůzce),*
- *kyberstalking a stalking (nebezpečné pronásledování s použitím ICT),*
- *rizika sociálních sítí (zejména sítě Facebook),*
- *hoax a spam,*
- *zneužití osobních údajů v prostředí elektronických médií.“* [16]

„Základním východiskem činnosti projektu je terénní práce s nejrůznějšími cílovými skupinami, přednášková činnost, preventivní vzdělávací akce apod. Přednášky/besedy mapují jak konkrétní nebezpečné jevy, tak možnosti prevence a obrany proti útočníkům. Představa o problematice je vytvářena na základě modelových situací i skutečných kauz. Besedy jsou multimediální, jsou doprovázeny prezentací a video ukázkami.“ [16]

„Mezi cílové skupiny projektu E-Bezpečí patří žáci a studenti (od 1. stupně ZŠ), učitelé, preventisté sociálně patologických jevů, metodici prevence, policisté (městská policie, Policie ČR), manažeři prevence kriminality, vychovatelé, pracovníci OSPOD a v neposlední řadě také rodiče.“ [16]

„Kromě vzdělávacích akcí realizuje projekt E-Bezpečí také pravidelná celorepubliková výzkumná šetření, zaměřená na rizikovou komunikaci v online prostředích, provozuje také online poradnu, vydává řadu zajímavých tiskovin pro žáky/učitele a realizuje řadu dalších aktivit.“ [16]

3.3.2 Odbor prevence městské policie Brno

„Odbor prevence Městské policie Brno je výkonný a metodický organizační celek s celoměstskou působností, který plní úkoly při zabezpečování místních záležitostí veřejného pořádku.“ [17]

„Přispívá k ochraně bezpečnosti osob a majetku v souladu se zák. 553/1991 Sb., o obecní policii, v platném znění, a to zejména přípravou a realizací projektů prevence kriminality, dopravní nehodovosti a sociálně patologických jevů.“ [17]

ZÁVĚR

Internetové sociální sítě mohou být užitečným nástrojem, který uživateli umožní kontakt s lidmi, který by v opačném případě bylo těžké zrealizovat. Existuje mnoho realizací implementace, kdy každá z nich poskytuje v podstatě podobné funkce s možnou specializací na určitou skupinu uživatelů. Tato práce se skládá z teoretické části, kde jsem popsal základní vymezení pojmů, historií, možnostmi využití a popisem nejvyužívanějších českých a zahraničních aplikací. Následuje analýza vnějších hrozeb a vnitřní zranitelnosti spolu s určením jejich velikosti a nezbytného návrhu opatření, které zajistí jejich minimalizaci. Z analýzy vyplynula důležitá fakta. Především se jedná o možné riziko zneužití sociálních sítí útočníky, kdy je přímo či nepřímo ohrožen majetkový, fyzický a psychický stav obětí. Tato rizika se týkají všech věkových skupin, přičemž nejvíce je ohrožena nejmladší generace, tedy děti a mladiství. Nejvíce zranitelným článkem každého systému je přitom sám uživatel. Důsledkem analýzy je tedy návrh bezpečnostních opatření, jejichž dodržování uživateli zaručuje minimalizaci zneužití bezpečnostních rizik. Lidé si velmi často ani neuvědomují, že je to pouze jejich chování, které určuje míru bezpečnosti na sociálních sítí. Dle uvedeného výzkumu se jedná především o lidi mladší 25 let. Můj další návrh se tedy týká integrace výuky o internetové bezpečnosti do systému školství. Existují sice různé organizace, jejichž posláním je pomoc a prevence proti těmto rizikům, avšak účinnost není velká, jelikož se jedná většinou o neziskové organizace a není v jejich silách informovat veškerou širokou veřejnost. Právě z toho důvodu je potřeba integrace do systému školství nezbytná. Nejdůležitější bezpečnostní opatření je vždy prevence. Pokud se uživatelé dokáží vyhnout a předcházet bezpečnostním rizikům, pak sociální sítě mají potenciál sloužit jako velmi užitečný nástroj poskytující v podstatě neomezené možnosti komunikace a tvorby vazeb mezi uživateli. Můj další návrh vyplývající z analýzy se pak týká samotných provozovatelů aplikací sociálních sítí. Nikdy nelze mluvit o bezpečném pohybu na komuntích webech, pokud nebudou dodrženy mnou navržené body, které by jej měly zajistit. Důkazem budiž zvyšující se internetová kriminalita, přičemž pravděpodobně neexistuje ze zjevných marketingových důvodů vůle provozovatelů sítí integrovat striktní bezpečnostní politiku.

ZÁVĚR V ANGLIČTINĚ

Internet social networks may be a useful tool which allows the user to contact with people which would otherwise be difficult to realize. There are many implementations, each of which provides substantially similar functions with possible specialization in a certain group of users. This work consists of a theoretical part where I described the basic definitions, history and description of applications, most highly used by Czech and foreign applications. The following analysis of external threats and internal vulnerabilities along with an indication of their size and draft the necessary measures to ensure their minimization. The analysis revealed important facts. Above all it is a possible risk of abuse of social networking attackers when directly or indirectly threatened property, physical and mental condition of the victims. These risks relate to all age groups and is most threatened by the youngest generation, children and adolescents. Most vulnerable is the article of each system while the user himself. The consequence analysis is therefore a proposal of security measures to ensure compliance with the user to minimize the security risks of abuse. People often do not even realize that it is only their behavior that determines the level of safety on social networking sites. According to the research is primarily about people younger than 25 years. My next proposal therefore relates to the integration of teaching about Internet safety in the school system. Although there are a variety of organizations whose mission is to help and prevent these risks, but efficiency is not great, since they are mostly non-profit organization and is not in their power to inform the entire public. It is for this reason, the need for integration into the education system is necessary. The most important safety measure is always prevention. If users are able to avoid and prevent security risks, the social networks have the potential to serve as a very useful tool that provides almost unlimited possibilities of communication and links between users. My next proposal from the analysis concerns itself with the operators of social networking applications. Never can not speak for the safe movement komuntích sites unless they comply with the proposed points me that it should deliver. Witness the growing Internet crime, which may not exist for obvious marketing reasons, network operators will integrate a strict security policy.

SEZNAM POUŽITÉ LITERATURY

[1] Fakulta informatiky a managementu Univerzita Hradec Králové *uhk.cz* [online]. [cit. 2011-08-25]. Ochrana a bezpečnost dat - terminologie. Dostupné z WWW: <http://security.uhk.cz/page.aspx?page_id=37&mode=1&letter=20>.

[2] Wikipedie.cz *wikipedie.cz* [online]. [cit. 2011-08-25]. Sociální síť. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Sociální_síť>.

[3] Facebook tiskové středisko facebook.*com* [online]. [cit. 2011-08-29]. Tiskové zprávy. Dostupné z WWW: <http://www.facebook.com/press.php>.

[4] Wikipedie.cz *wikipedie.cz* [online]. [cit. 2011-08-29]. Facebook. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Facebook>.

[5] Wikipedie.cz *wikipedie.cz* [online]. [cit. 2011-08-30]. Twitter. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Twitter>.

[6] Wikipedie.cz *wikipedie.cz* [online]. [cit. 2011-08-30]. LinkedIn. Dostupné z WWW: <http://cs.wikipedia.org/wiki/LinkedIn>.

[7] IndexTrade *indextrade.cz* [online]. [cit. 2011-09-02]. Web 2.0 jako důležitý milník v evoluci webu. Dostupné z WWW: <http://www.indextrade.cz/clanky/web-20-jako-dulezity-milnik-v-evoluci-webu>.

[8] BUREŠ, L. Internetové sociální sítě, pohled na jejich využívání především žáky ZŠ a s tím spojená případná rizika. Brno, 2010. 83 s. Diplomová práce na Pedadgogické fakultě Masarykovy Univerzity na katedře technické a informační výchovy. Vedoucí diplomové práce Ing. Martin Dosedla.

[9] JAISHANKAR, Karuppannan. Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. 1st printing, 2011. Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India. 461 s. ISBN 978-1-439-82949-3.

[10] JIROVSKÝ, Václav. Kybernetická kriminalita. 1. vydání, 2007. Grada; Praha. 240s. ISBN 80-247-1561-9.

[11] Google, Inc. *google.com* [online]. [cit. 2011-09-12]. Nejčastější dotazy týkající se ochrany osobních údajů – Centrum pro ochranu osobních údajů Google. Dostupné z WWW: <http://www.google.com/intl/cs/privacy/faq.html#toc-terms-personal-info>.

[12] Richard Šimek, Faklulta informatiky, Masarykova univerzita Brno. *muni.cz* [online]. [cit. 2011-09-15]. Sociotechnika (sociální inženýrství) - kolokviální práce do předmětu PV109 Dostupné z WWW: < http://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm>.

[13] Seznam.cz. *firma.seznam.cz* [online]. 2009 [cit. 2011-08-11]. O firmě. Dostupné z WWW: <http://firma.seznam.cz/cz/historie-firmy.html>.

[14] Seznam.cz. *seznam.cz O nás* [online]. [cit. 2011-08-11]. Spolužáci.cz. Dostupné z WWW: <http://firma.seznam.cz/cz/spoluzaci-cz.html>.

[15] Cnews. *cnews.cz* [online]. [cit. 2011-10-01]. Desatero bezpečnostních přikázání. Dostupné z WWW: <http://www.cnews.cz/desatero-bezpecnostnich-prikazani>.

[16] Projekt e-bezpečí.cz. *e-bezpeci.cz* [online]. [cit. 2011-10-04]. Informace o projektu. Dostupné z WWW: <http://www.e-bezpeci.cz/index.php/o-projektu/oprojektu>.

[17] Městská policie Brno. *mpb.cz* [online]. [cit. 2011-10-04]. Městská policie Brno – odbor prevence. Dostupné z WWW: <http://www.mpb.cz/odbor-prevence/>.

[18] TechNet.cz. *technet.cz* [online]. [cit. 2011-10-01]. Češi Facebooku nebezpečně věří. Falešné krasavici naletělo 60 procent. Dostupné z WWW: <http://technet.idnes.cz/cesi-facebooku-nebezpecne-veri-falesne-krasavici-naletelo-60-procent-112-/sw_internet.aspx?c=A091117_171036_sw_internet_pka>.

[19] SC Magazine. *scmagazineus.com* [online]. [cit. 2011-10-10]. Facebook bloggers reveal way to peek at private profiles. Dostupné z WWW: <http://www.scmagazineus.com/facebook-bloggers-reveal-way-to-peek-at-private-profiles/article/138867/>.

[20] The Univestiy of Alabama. *ua.edu* [online]. [cit. 2011-09-23]. ABC's of Eductation: Cyberbullying. Dostupné z WWW: <http://www.ua.edu/features/abcsofeducation/cyberbullying.html>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IRC	Internet Relay Chat – protokol pro komunikaci na internetu v reálném čase.
OSPOD	Orgán sociálně-právní ochrany dětí.
CRM	Customer relationship management – řízení vztahů se zákazníky.

SEZNAM OBRÁZKŮ