Internet, bezpečnost a konkurenceschopnost organizací
16. – 17. března 2011, Univerzita Tomáše Bati ve Zlíně

SOCIÁLNÍ SÍTĚ A VIRTUÁLNÍ SVĚTY – HROZBA PRO FIRMY?

SOCIAL NETWORKS AND VIRTUAL WORLDS – A THREAT TO ORGANIZATIONS?

Klára BENDOVÁ, Jaroslava KUBÁTOVÁ
Katedra aplikované ekonomie, FF UP v Olomouci, Křížkovského 12, 771 80 Olomouc, ČR,
klara.bendova@upol.cz, jaroslava.kubatova@upol.cz

Anotace: *Příspěvek dokládá, že uživatel internetových aplikací, např. sociálních sítí nebo virtuálních světů je vystaven řadě rizik. Sociální sítě i virtuální světy jsou lákavými prostředími pro sociotechniky. Na příkladech ukazujeme, jak snadno se uživatelé vystavují zneužití své identity. Jedním z fenoménů virtuálního prostředí je např. vystupování uživatelů pod opačným pohlavím (gender swapping). Příspěvek je doplněn o výsledky průzkumu názorů studentů KAE FF UP na dané téma. Ze zjištění vyplývá, že pro bezpečnost organizací je nutno řádně proškolit zaměstnance o možných rizicích na sociálních sítích.*

Abstract: *The paper highlights that the users of internet applications, like social networks or virtual worlds, are put at several risks. Social networks as well as virtual worlds are tempting backgrounds for sociotechnics. We demonstrate at the examples how easily the users put their identities in jeopardy. One of virtual environment phenomena is for example the gender swapping of the users. The paper is extended by the results of our research on this theme among the students of the Department of Applied Economics at Palacký University. The results prove how important is to train the employees to keep the organizational data secure.*

Klíčová slova: *Důvěra, sociotechniky, virtuální prostředí*

Keywords: *Trust, sociotechnics, virtual environment.*

1. Rozsah a obsah sociálních sítí

Zdánlivě nevinná aktivita, jakou je využívání internetových sociálních sítí k posilování mezilidských vztahů a ke sdílení znalostí, je bezpečnostní hrozbou nejen pro samotné uživatele, ale i pro jejich zaměstnavatele. Nejprve posuďme, jak rozšířené je užívání sociálních sítí na internetu. Sociální síť je soubor vztahů; formálněji řečeno, síť obsahuje objekty (zvané též uzly, nodes) a zobrazuje (popisuje) vztahy mezi objekty.[10] Objekty jsou jednotlivci, popř. organizace. Pokud máme na mysli sociální sítě na internetu, jedná se o kombinaci webhostingové služby a specializovaného vyhledavače. Uživatel se na síť přihlásí (vytvoří si účet), vytvoří si strukturovaný profil a okamžitě může hledat jiné uživatele a být nalézán.

Počty uživatelů internetu i sociálních sítí se rychle vyvíjejí. Na přelomu let 2010 a 2011 překročil počet uživatelů internetu ve světě 2 miliardy, to znamená, že se penetrace internetu celosvětově blíží 30 %.[6] Podle mezinárodního průzkumu společnosti InSites Consulting [1] z roku 2010 zná 90 % uživatelů internetu alespoň jednu sociální síť. Nejproslulejší je Facebook, který zná 73 % uživatelů internetu. Aktivními uživateli sociálních sítí je 72 % uživatelů internetu a 28 % uživatelů není členem žádné sociální sítě, ovšem třetina z těchto ne-uživatelů měla v plánu na sociální síť vstoupit. Uživatelé jsou v průměru členy dvou sociálních sítí, přičemž nejpoužívanějšími jsou Facebook, kde má účet 51 % uživatelů sítí, dále MySpace s 20 % uživatelů a Twitter se 17 % uživatelů. Nejpopulárnější sociální síť Facebook má řádově 400 milionů aktivních uživatelů, z toho polovina se přihlašuje denně, 100 mil. využívá přístup přes mobilní telefon. Průměrný počet přátel jednoho uživatele Facebooku je 130 [5], přičemž průměrný počet přátel na všech sociálních sítích je 195. Významná profesionální sociální síť LinkedIn má přes 65 milionů členů, což je 9 % celkového počtu uživatelů.[8]

Základními dvěma důvody, proč lidé do sociálních sítí vstupují, je jednak osobní využití, tedy budování přátelských kontaktů a sdílení osobních informací, a jednak profesní, to znamená budování kontaktů na základě odbornosti, popř. zaměstnání s cílem budování znalostních sítí. V praxi výrazně převažuje užívání pro osobní účely, 84 % uživatelů je členy pouze privátních sítí, 13 % uživatelů je členy jak osobní sítě, tak profesní sítě a jen 3 % uživatelů jsou jen na profesní síti. Co se týká četnosti vstupů, uživatelé na svou síť vstupují průměrně 2x denně, ale uživatelé profesních sítí se na svůj účet přihlašují v průměru pouze 9x měsíčně. Nejobvyklejšími aktivitami, kterým se lidé na sítích věnují, jsou:

- odesílání osobních zpráv,
- prohlížení obrázků (fotografií),
- kontrola/úprava vlastního statusu,
- reakce na status jiných účastníků,
- nahrávání obrázků (fotografií).

Mnozí uživatelé sociálních sítí zveřejňují riskantní údaje.[9]. Více než polovina uživatelů (52 %) uvádí úplná data narození, pětina uživatelů (21 %) vystavuje fotografie svých dětí a uvádí i jejich jména (13 %). Osm procent uživatelů uvádí adresu trvalého bydliště a tři procenta uživatelů na síti sdělují, kdy opouštějí domov. Naivitu uživatelů sociálních sítí lze ilustrovat příkladem z Facebooku. Pokus provedla bezpečnostní firma Sophos v roce 2007.[12] Pracovníci firmy vytvořili na Facebooku účet žabáka jménem Freddi. Freddi rozeslal 200 nabídek přátelství, přičemž potvrzení přátelství znamená umožnění přístupu k důvěrnějším osobním údajům, a akceptováno bylo 82 nabídek, tedy 41 %. Profil Freddieho[1] je na obrázku 1.

Obr. 1: Profil Freddieho

V současnosti je již ochrana soukromí na Facebooku propracovanější než v uvedeném roce, ovšem část uživatelů si neumí profil správně nastavit anebo se chová lehkomyslně. Autorky znají z vlastního okolí nedávný případ, kdy jeden uživatel rozesílal nabídky přátelství z profilu Falešný Účet. Mnoho jich bylo přijato… Profily s názvy, které neobsahují jméno a příjmení, byly provozovateli Facebooku na přelomu let 2010 a 2011 odstraněny, ovšem to situaci nijak nezlepšuje, neboť na sociálních sítích nelze ověřit skutečnou identitu uživatelů.

2. Social Media Knowledge Worker

Zaměstnavatelé si musí uvědomit, že dnes do jejich společností přicházejí pracovat lidé, kteří patří k takzvané Digitální generaci. Digitální generaci tvoří mladí lidé, Digital Natives, kteří vyrostli v digitalizovaném prostředí, to znamená, že měli od dětství přístup k internetu a dalším nástrojům vzdálené komunikace. Tito lidé jsou považováni (a vesměs právem) za velmi zdatné uživatele informačních a komunikačních technologií.[3] Podle prognóz tito Digital Natives během pěti let na pracovištích početně převýší

[1] K 10. 2. 2011 na Facebooku tento profil není.

generaci tzv. Baby Boomers, tj. lidí narozených v letech 1945 – 1965. O vzdělaných Digital Natives se také hovoří jako o Social Media Knowledge Workers, což vyjadřuje jejich sklon používat ke znalostní práci právě i sociální média, resp. sociální sítě. Jednou z významných odlišností těchto mladých pracovníků je například neochota využívat ke komunikaci e-maily, což je jinak nejfrekventovanější nástroj sdílení znalostí. Social Media Knowledge Workers komunikují prostřednictvím sociálních sítí a jiných aplikací Webu 2.0. Ostatně i společnosti se tomuto trendu přizpůsobují a například pro získávání pracovníků užívají stále častěji sociální sítě, obzvláště využívaný je pro tuto aktivitu Linkedin.

Obr. 2: Vývoj komunikace [4]

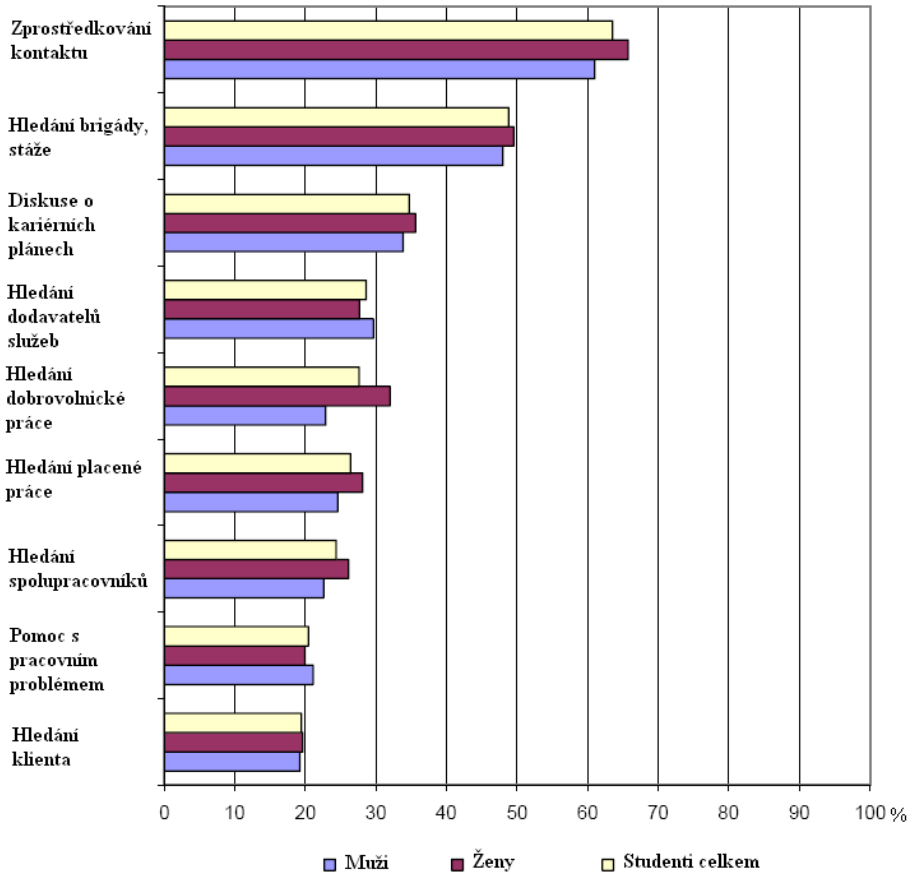
Mezinárodní studentská organizace AIESEC provedla ve spolupráci s The Career Innovation Company průzkum komunikačních a pracovních stylů Digitální generace.[13] Průzkum byl realizován v roce 2008 mezi 2 277 studenty ze 114 zemí a 530 zaměstnanci z 83 zemí.

Na 80 % studentů využívá Instant messaging, více než polovina přes internet telefonuje, tři čtvrtiny studentů mají profil na sociální síti a polovina hraje on-line hry. Skoro čtvrtina studentů, 23 %, má i virtuální život v některém z internetových virtuálních světů. Jak vyplývá z tabulky 1, využívání technologií se mezi studenty a již zaměstnanými respondenty výrazně neliší. Sítí, kde má profil nejvíce studentů, je Facebook, zaměstnanci pak nejčastěji využívají Linkedin.

	Studenti		Zaměstnanci	
Procentní podíl využití technologií pro:	Učení se	Socializaci	Práci	Socializaci
Vyhledávání a publikování informací	94%	99%	88%	98%
Komunikace one-to-one	96%	98%	97%	98%
Simulace a hraní her	17%	63%	10%	56%
Spolupráce	89%	93%	91%	89%
Publikování myšlenek (např. na blogu)	26%	63%	25%	55%

Tab. 1: Využívání technologií pro různé účely – srovnání studentů a zaměstnanců

Studenti využívají technologie k moha účelům, spjatých s prací a se studiem. Percentuální podíly studentů (členěno i dle pohlaví), které využívají sociální sítě k uvedeným účelům, zobrazuje graf 1.



Graf 1: Využívání sociálních sítí pro různé účely

3. Rizika networkingu a jejich minimalizace

V současnosti tedy není otázka, zda by společnosti měly užívání sociálních sítí povolit, otázka je, jak to udělat co nejlépe. Užívání sociálních sítí ze strany pracovníků má mnoho výhod a mnoho úskalí. Mezi hlavní výhody můžeme zařadit nízké náklady na navázání a udržení pracovních vztahů s lidmi, kteří by jinak byli nedostupní, přístup k širokému okruhu znalostních pracovníků či diverzita komunikujících osob, což podporuje tvůrčí a inovativní přístupy k řešeným úkolům. Mezi nevýhody patří zejména ohrožení soukromí a směšování pracovního a osobního života. Nelze nezmínit ani vliv sociálních médií na utváření pověsti firem. Dále se budeme zabývat hrozbami, které sociální networking pro firmy představuje.

V roce 2009 převýšil celosvětově rozsah komunikace prostřednictvím sociálních sítí komunikaci e-mailovou. Komunikace prostřednictvím sociálních sítí, resp. aplikací Webu 2.0 je ale spjata s řadou rizik. Podle odhadů je 65 % těchto rizik spjato s botnety a malwarem, další více než třetina problémů je spjata s lidským chováním. Každopádně, organizace musí zaměstnávat dostatečně kompetentní odborníky, kteří dobře rozumí nejmodernějším komunikačním technologiím. Tito odborníci by se měli zaměřit na následující čtyři klíčové oblasti, aby zajistili bezpečnost organizací: eDiscovery, Data protection, Perimeter a Compliance.[11]

eDiscovery

eDiscovery spočívá ve vyhledávání, procházení, umisťování a zajišťování dat pro právní případy. Sociální sítě užívají různé metody shromažďování obsahu. I když profesionální sociální networking může být prospěšný pro výkon organizace. Řada společností není připravena tuto oblast v rámci eDiscovery dobře řešit, a tím se vystavuje zbytečnému riziku. Minimem, které mohou společnosti udělat, je proškolit své zaměstnance, jak

sociální sítě používat, a stanovit jasnou politiku, jak mají zaměstnanci vystupovat na sociálních sítích jako reprezentanti firmy a důsledně odlišit tuto komunikaci od soukromých mimopracovních aktivit. Extrémním řešením je zákaz (zablokování) přístupu k sociálním sítím z pracovních počítačů. Takové rozhodnutí ale není v souladu se současnými trendy sdílení znalostí a může být pro firmu kontraproduktivní.

Data protection

Z hlediska ochrany dat je třeba přemýšlet o technických aspektech a o lidském faktoru. Technické řešení spočívá zpravidla v šifrování dat a v nástrojích na ochranu jejich zcizení. Veliké riziko ovšem představuje lidský faktor. I taková drobnost, kdy pracovník na soukromém profilu (např. na Facebooku) napíše zprávu, na čem pracuje, může ohrozit konkurenceschopnost organizace. Podobně, jakékoliv negativní zprávy o zaměstnavateli na profilech zaměstnanců poškozují dobré jméno firmy. Samozřejmě, každá firma se má k zaměstnancům chovat tak, aby neměli důvod psát negativní informace, ale v reálném životě dennodenních pracovních kontroverzí může pracovník impulsivně vyvěsit zprávu, která odráží jeho aktuální emocionální stav, přičemž interpretace této zprávy může mít velmi negativní dopady. Řešením je opět důsledné vzdělávání zaměstnanců a vyžadování osobní odpovědnosti za chování na sociálních sítích. Porušení stanovených pravidel musí mít jednoznačně stanovené důsledky.

Perimeter

Bezpečnostní perimeter je fyzická nebo logická hranice informačního systému, od níž je realizována bezpečnostní politika a bezpečnostní opatření. Obvyklým nástrojem je firewall. Společnosti navíc nezřídka blokují přístup z proxy serverů k sociálním sítím, aby nevystavily data z těchto serverů jakémukoliv nebezpečí. Ani v tomto případě ale nelze opominout sociální a fyzické počiny člověka. Jako je nutné nenechávat na pracovních stolech materiály s důvěrnými daty, tak je důležité zodpovědně nakládat s daty v elektronické podobě. Technicky i personálně je tedy nutno zajistit bezpečné chování personálu uvnitř i za hranicemi perimetru.

Compliance

Pod pojmem compliance máme na mysli soubor opatření, kterými lze dosáhnout, popř. vynutit, dodržování stanovených bezpečnostních pravidel. Každý zaměstnanec musí mít jasně stanovenou, kontrolovatelnou a hodnotitelnou odpovědnost za data, s nimiž přichází do kontaktu. Užívání sociálních médií přináší na zavádění těchto opatření stále nové nároky, takže musí být průběžně aktualizována tak, jak se vyvíjejí webové aplikace.

Sociální média jsou navíc prostředím, které přitahuje sociotechniky. Projevuje se zde tzv. opportunity effect: zvýšené množství příležitostí ke kriminálním činům vyvolává růst kriminality.[2] Sociální sítě jsou obzvláště lákavé pro nasazení tzv. techniky podvodných vztahů. Podvodné vztahy jsou od počátku navazovány s cílem využít oběť. Vztah se může zakládat např. na sdílení společných zájmů, názorů či nalezení „společného nepřítele“. Velmi úspěšnou variantou podvodného vztahu je vytvoření dojmu vzájemné podobnosti, tedy že oběť a útočník mají podobné životní zážitky a zkušenosti, podobné zájmy a hodnotové systémy a způsoby myšlení. Přesvědčení, že někdo má podobné charakteristiky jako my, velmi posiluje naši ochotu jednat ve prospěch této osoby a důvěřovat jí, aniž bychom k tomu měli objektivní důvod. Je zřejmé, že k použití této taktiky velmi napomáhají sociální sítě, uživatelé tu na svých profilech uvádějí údaje, z nichž lze snadno zjistit mnoho informací, jimž se pak útočník „připodobní“ oběti. Sociální síť je zjevně ideálním místem, kde podvodný vztah může „náhodou“ začít.

Pro přiblížení, jak málo důvěryhodná komunikace na sociálních sítích může být, uvedeme příklad tzv. genderswappingu. Pod pojmem genderswapping rozumíme vystupování uživatele sociální sítě pod opačným pohlavím, než je jeho biologické pohlaví. Podle odhadů 54 % mužů a 68 % žen buď uvažuje o vytvoření anebo si již vytvořilo na sociální síti, popř. v on-line hře, profil (avatara) opačného pohlaví. Důvodů tohoto chování je řada, počínaje pouhou zvědavostí, přes řešení problémů s vlastní reálnou identitou, až po záměrnou manipulaci s ostatními uživateli nebo získání určité výhody.[7] Uživatelé, vystupující pod ženskou identitou uvádějí, že s nimi uživatelé vystupující pod mužskou identitou jednají lépe, než když jedná virtuální muž s virtuálním mužem. Virtuální muži jsou k virtuálním ženám vlídnější, mírnější, jsou ochotni jim radit a pomáhat, popř. jim dávat (v případě her či virtuálních světů) dárky. Virtuální muži s virtuálními ženami flirtují, bohužel se dopouštějí i sexual harassmentu či sledování vyhlédnutých obětí, a to často s cílem zjistit reálnou identitu (skutečné pohlaví a věk) uživatelky.

Na Univerzitě Palackého v Olomouci jsme provedli průzkum názorů u studentů Katedry aplikované ekonomie na téma budování důvěry a práce ve virtuálním prostředí. Studenti se účastnili výuky v předmětu Virtual Work, kde aktivně po dobu jednoho semestru pracovali ve virtuálním prostředí Second Life. Každý ze

studentů vlastnil svého Avatara v SL. Dle zjištění, někteří ze studentů se ve virtuálním prostředí pohybují pravidelně i mimo výuku. Většina respondentů měla s virtuálním prostředím bohaté zkušenosti. Někteří využívali virtuální prostředí i pro pracovní účely. Ze sociálních sítí studenti nejčastěji využívají Facebook a Twitter. V průzkumu se autorky zabývaly otázkou, zda je možné ve virtuálním prostředí budovat důvěru. Zaměřily jsme se na budování důvěry v pracovním kolektivu respektive podporu týmové práce. Výsledky naznačují, že i ve virtuálním prostředí, bez znalosti druhé osoby face-to-face, lze vybudovat kvalitní interpersonální vztahy. Většinou se však také potvrzuje, že potkají-li se osoby v reálném světě, výrazně to podpoří a urychlí budování vzájemné důvěry. Zajímavé je, že zejména respondenti, kteří měli bohatší zkušenosti s virtuálním prostředím, byli vůči budování důvěry a navazování interpersonálních vztahů mnohem ostražitější, než respondenti, kteří virtuální prostředí dříve tolik nevyužívali. Obecně lze konstatovat, že studenti KAE FF UP podporují názor, že i ve virtuálním prostředí bez kontaktu face-to-face je možné navázat „vztah“ a získat vůči druhé osobě (Avatarovi) plnou důvěru, což vede ke sdílení informací. Důvěra a sdílení informací ve virtuálním prostředí bohužel přinášejí i rozsáhlé možnosti ke zneužití společností i jednotlivci.

4. Závěr:

Rozvoj sociálních sítí, resp. sociálního networkingu je nezastavitelný. Možnost komunikace prostřednictvím sociálních sítí, mezi něž patří i virtuální světy, jako např. Second Life, je velkou příležitostí pro firmy, které využívají znalostní práci. Na druhou stranu se s užíváním sociálních sítí pojí velká a obtížně eliminovatelná rizika. Tato rizika jsou jak technického rázu, tak sociálního rázu. Firmy musí na rozvoj virtuální komunikace reagovat jak správným technickým zabezpečením svých dat, tak důslednou politikou užívání sociálních sítí, školením zaměstnanců a vymezením a vymáháním osobní odpovědnosti každého uživatele.

Literatura

[1] Bellegham van, S.: Social Media aroun the World: Retrieved March 29, 2010 from <http://www.slideshare.net/InSitesConsulting/social-media-around-the-world-3547521>.

[2] Crime and the Economy. Research conducted by the Police Federation of England and Wales. May 2009. Retrieved April 4, 2010 from <http://www.polfed.org/Crime_and_the_economy_paper_(2).pdf>.

[3] Hargittai, E: Digital Na(t)ives? Variation in Internet Skills and Uses among Members of the ‘‘Net Generation’’. Sociological Inquiry, Vol. 80, No. 1, February 2010, 92–113.

[4] <http://jeffreyhill.typepad.com/english/2009/03/cartoon-the-evolution-of-communication.html>, Retrieved January 17, 2011.

[5] <http://www.facebook.com/press/info.php?statistics>, Retrieved January 29, 2011.

[6] <http://www.physorg.com/news/2011-01-internet-users-worldwide-billion.html>, retrieved January 9, 2011.

[7] <http://www.slideshare.net/Facegroup/women-myths-and-video-games>, retrieved February 7, 2011.

[8] <http://www.slideshare.net/stevenvanbelleghem/social-networks-around-the-world-2010>, retrieved February 4, 2011.

[9] <http://www.tgdaily.com/security-features/49619-most-social-network-users-court-cybercrime-says-report>, retrieved February 7, 2011.

[10] Kadushin, Ch.: Introduction to Social Network Theory. Retrieved March 29, 2010 from <http://home.earthlink.net/~ckadushin/Texts/Basic%20Network%20Concepts.pdf>.

[11] Sizemore, Heft: Examining the 4 Areas of Business Social Networking Risk. Retrieved March 29, 2010 from <http://www.cioupdate.com/insights/article.php/3887541/Examining-the-4-Areas-of-Business-Social-Networking-Risk.htm>.

[12] Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves. Retrieved March 29, 2010 from <http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html>.

[13] The digital generatoin survay. Retrieved March 29, 2010 from <http://www.slideshare.net/guest50fdb1/digital-generation-survey-2008-technology-part-1-presentation>.