Strategie manipulace dětí v online prostředích se zaměřením na tzv. kybergrooming

Mgr. Kamil Kopecký, Ph.D.
Centrum prevence rizikové virtuální komunikace, Pedagogická fakulta UP v Olomouci

Příspěvek se zaměřuje na vybrané strategie manipulace dětí v online prostředích se zaměřením na tzv. *kybergrooming*. Termínem kybergrooming označujeme chování uživatelů internetu, které má přimět vyhlédnutou dětskou oběť k osobní schůzce v reálném světě (výsledkem schůzky může být sexuální zneužití, fyzický útok, pořizování dětské pornografie, dětská prostituce apod.). Příspěvek se zaměřuje na vybrané techniky, které se k útokům na děti využívají, popisuje rovněž vybrané případy, v rámci kterých byly techniky útoku zneužity.

Klíčová slova: kybergrooming, zneužití dítěte, kybernetická kriminalita, webcam trolling.

The strategies of child manipulation in online environments with a focus on cyber grooming

Cyber grooming (child grooming, grooming) represents the Internet users' behaviour (predators, cyber groomers) which is supposed to raise false confidence and make victim come to a secret personal meeting. The sexual abuse of the victim, physical violence or child prostitution and pornography abuse might be the results of this rendezvous which means that cyber grooming is a kind of psychological manipulation carried out through the internet, mobile phones and other relevant technologies. The paper also focuses on examples of manipulation connected with attacks to children. The last part of paper describes featured cases of cybergrooming.

Key words: kybergrooming, child abuse, cybercrime, webcam trolling.

Úvod do problematiky

Termín *kybergrooming* (child grooming, grooming) označuje chování uživatelů internetu (predátorů, kybergroomerů), které má v oběti vyvolat falešnou důvěru a přimět ji k osobní schůzce (Kopecký, 2010). Výsledkem této schůzky může být sexuální zneužití oběti, fyzické násilí na oběti, zneužití oběti pro dětskou prostituci, k výrobě dětské pornografie apod. Kybergrooming je tedy druhem psychické manipulace realizované prostřednictvím internetu, mobilních telefonů a dalších souvisejících technologií (1, 2, 3).

Kybergrooming je často vázán na synchronní i asynchronní komunikační platformy, nejčastěji veřejný chat, internetové seznamky, instant messengery a VoIP (např. ICQ, Skype) a v posledních letech také na sociální sítě (Facebook, Ask.fm, Lidé.cz a další). Podle řady výzkumů (4) probíhá kybergrooming nejčastěji právě v prostředí instant messengerů (56 % případů), další pozici pak obsadily sociální sítě (11,4 % případů).

Lze však předpokládat, že počet případů kybergroomingu probíhajícího s použitím sociálních sítí několikanásobně vzrostl. Internetoví predátoři však kromě těchto komunikačních prostředí využívají také inzertní portály, na kterých nabízejí dětem různé možnosti výdělku či kariéry (např. v oblasti modelingu), často navštěvují portály zaměřené přímo na nezletilé uživatele internetu (dětské portály, portály zaměřené na volnočasové aktivity, herní portály a další internetové stránky).

Psychická manipulace v rámci kybergroomingu probíhá obvykle delší dobu – od cca 1 měsíce po dobu několika let. Tato doba je přímo závislá na způsobu manipulace a na důvěřivosti oběti. Existují případy, kdy predátor manipuloval dítě po dobu 2 let, než došlo k osobnímu setkání a sexuálnímu zneužití či znásilnění (5).

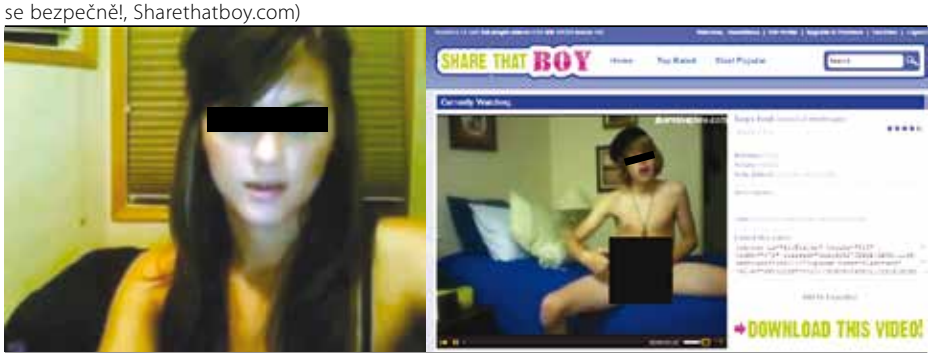
Zaměříme-li se na diagnostiku útočníků, jedná se (dle sociálního statutu) o heterogenní skupinu, ve které nalezneme uživatele jak s nízkým, tak i vysokých sociálním statutem. V řadě případů oběť pachatele zná a je na něm závislá (v 85–95 % případů) (6). Mezi útočníky převažují dle výzkumů osoby, které dosud nebyly trestány, útočníky se však někdy stávají i ti, kteří již byli za sexuální útoky proti dětem či mladistvým odsouzeni a došlo u nich k recidivě (7). U části z útočníků (sexuálních abuzérů) byla diagnostikována deviace či porucha sexuální preference (pedofilie, hebofilie, efebofilie). Nelze však ztotožňovat termín *pedofil* a *sexuální abuzér* (8, 9).

V českých podmínkách se často *kybergrooming* spojuje s termínem *sociální inženýrství*, pro potřeby tohoto textu však oba termíny odlišujeme. Sociální inženýrství vnímáme jako soubor strategií, jak manipulovat uživatelem internetu, jak od něj získávat osobní údaje a další citlivé materiály apod. Sociální inženýrství je tedy jakýmsi souborem technik a strategií. Primárním cílem sociálního inženýrství není sexuální zneužití dítěte či dospělého, sociální inženýrství může být zaměřeno např. na průnik na bankovní účet, na získání utajovaných informací atd. Kybergrooming je pak proces, který využívá technik sociálního inženýrství k tomu, aby donutil oběť dorazit na osobní schůzku, přičemž primárním cílem kybergroomingu je sexuální zneužití oběti.

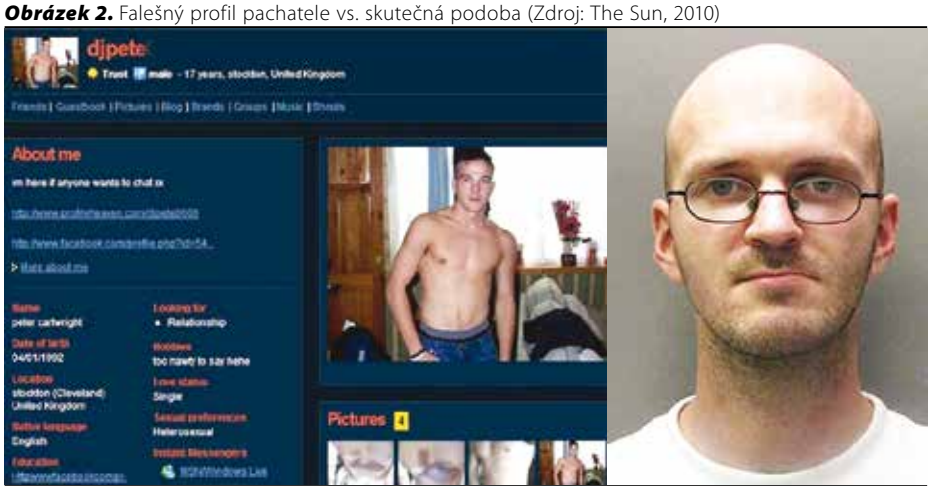
Vybrané techniky manipulace a kontaktování oběti

V procesu manipulace v rámci kybergroomingu se uplatňuje řada technik, které jsou

Obrázek 1. Webcam trolling (vlevo podvržený záznam, vpravo získaný záběr) (Zdroj: E-Bezpečí, Seznam se bezpečně!, Sharethatboy.com)



Obrázek 2. Falešný profil pachatele vs. skutečná podoba (Zdroj: The Sun, 2010)



Graf 3. Odsouzení Milan Machát a Martin Mertl (vpravo) (Zdroj: MAFRA, 2013)

zaměřeny na získání důvěry dítěte, ovlivnění jeho chování a následnou manipulaci, jejímž cílem je přinutit dítě k osobní schůzce. U jednotlivých ofenzivních technik uvádíme jejich stručnou charakteristiku, techniky a metody útoku jsou podrobně popsány např. v publikaci Nebezpečí internetové komunikace IV (5).

Vybrané techniky kontaktování dětí a manipulace

1. Technika „kobercového tapetování"

Základním principem techniky tzv. kobercového tapetování (10) je odfiltrování profilů konkrétních dětí v rámci zvolené sociální sítě a jejich následné hromadné oslovení útočníkem. V současnosti lze ve většině sociálních sítí vyhledávat uživatele podle více kritérií – např. věku, pohlaví, zájmů, lokality apod. Útočník tedy osloví děti hromadně, nabídne jim např. možnost komunikace, výměnu fotografií, nebo jim přímo nabídne zajímavou možnost výdělku. V prostředí českých i zahraničních sociálních sítí trvale roste množství dětí, které jsou ochotné za finanční obnos poslat útočníkovi svou vlastní intimní fotografii, video, případně svolí k sexuálnímu styku.

Jako jeden z příkladů dobrovolné dětské prostituce lze uvést kauzu teprve 12leté dívky z ČR, která v prostředí sociálních sítí nabízela sexuální služby. Nabízela však výhradně „rychlovky", které byla ochotna provádět od 7 do 8 hodin ráno (v 7 hodin odcházela její matka do práce a dívka zůstala v bytě hodinu sama). Díky poskytovaným sexuálním službám se jí podařilo získat hotovost ve výši více než 150 000,– Kč (11).

2. Strategie vylákávání intimních materiálů prostřednictvím fotografie osoby opačného pohlaví

Mezi další strategie, které se běžně využívají v rámci kybergroomingu, patří technika vylákávání intimních materiálů prostřednictvím fotografie osoby opačného pohlaví. Pokud tedy online predátor chce např. získat intimní fotografii chlapce, zahájí pod identitou fiktivní dívky komunikaci. Jakmile chlapec požádá o fotografii, útočník mu pošle fotografii dívky, která je alespoň částečně intimní (není vyloženě erotická, ale je na hraně intimity). Chlapec reaguje a zašle dívce obdobně laděné foto, útočník následně zašle chlapci více a více intimní materiály, chlapec reaguje a výsledkem je, že má útočník k dispozici fotografii obnaženého dítěte, kterou lze využít např. k vydírání (12).

3. Webcam trolling

Mezi další techniky útoku patří tzv. webcam trolling, tedy technika získávání intimních materiálů dětí i dospělých prostřednictvím podvržené videosmyčky, která je pomocí počítačového programu integrována do běžných aplikací či sociálních sítí, které umožňují videorozhovor (např. Skype, Facebook, G+ apod.). V praxi dítě vidí místo skutečného obrazu z videokamery podvržený videozáznam např. jiného dítěte. Videosmyčky ve většině případů neobsahují zvukovou stopu, proto také pachatelé dětem píší, že jim nefunguje mikrofon – že si tedy budou moci psát a vidět se na kameře, nicméně neuslyší se. Videosmyčky samozřejmě obsahují intimní fáze, přičemž cílem pachatele je donutit dítě, aby záznam napodobilo – následně jej nahrát a materiál využít k vydírání (13).

Mezi další techniky manipulace patří např. *mirroring* (zrcadlové napodobování komunikace dítěte), *luring* (vylákávání intimních materiálů prostřednictvím nabídky dárků), *phishing* (metoda získávání osobních údajů), *profilování obětí, techniky překonávání věkového rozdílu mezi útočníkem a obětí, techniky izolace oběti od okolí* apod.

Případy kybergroomingu (zahraničí)

Případ Peter Chapman (2010, Velká Británie)

Případ vraha Petera Chapmana představuje jeden z nejtragičtějších případů využití kybergroomingu k útoku na dítě na území Evropy, přičemž samotný pachatel byl v roce 2010 odsouzen k trestu odnětí svobody na doživotí (14).

Peter Chapman, třiatřicetiletý deviant, který byl již v minulosti odsouzen za znásilnění prostitutek, měl být po svém propuštění pod pravidelným dohledem policie. Od dubna roku 2008 se však policii přestal hlásit. Ta po něm vyhlásila celostátní pátrání až v září roku 2009, tedy měsíc před událostí, která stála život 17letou studentku ošetřovatelství Ashleigh Hallovou (15).

V rámci sociální sítě Facebook si Chapman vytvořil falešný profil (udal jméno Peter Cartwright a věk 19 let, nicméně měl vytvořeny i další profily). Pomocí Facebooku navázal kontakt se studentkou ošetřovatelství Ashleigh Hallovou, se kterou si po delší komunikaci domluvil schůzku. Tváří v tvář se jí představil jako otec jejího virtuálního přítele a na izolovaném místě nedaleko Sedgefieldu ji nejdříve znásilnil a pak zardousil (16). Chapmana policie zadržela během následujícího dne, kdy jej náhodou zastavila v souvislosti s podezřelou registrační značkou jeho auta. Chapman si totiž auto, které bylo policií evidováno v rámci jiného případu, zakoupil na aukčním serveru eBay – netušil, že auto figuruje v policejní databázi. Chapman se k vraždě dívky přiznal bezděčně, nepředpokládal, že jej policie zatkla za podezření ze spáchání vraždy.

Po zveřejnění kauzy začaly policii kontaktovat další dívky a také dospělé ženy, které se vizuálně podobaly zavražděné Ashleigh Hallové a které Chapman rovněž kontaktoval a snažil se je přimět k osobní schůzce (17).

Facebookový profil Chapmana obsahoval přes 3 000 virtuálních přátel = žen ve věkovém rozpětí 13–31 let. Osobní údaje od svých přátel získával také pomocí různých facebookových

dotazníků, ve kterých se ptal na velmi osobní otázky. Od některých dívek rovněž vylákal citlivé fotografie (ve spodním prádle, pyžamu apod.). Kromě Facebooku Chapman působil i na dalších sociálních sítích – Netlog, Holabox, Profileheaven, Kazoba apod. (18).

Použitá strategie útoku

Chapman využíval strategii falešné identity (falešný profil, falešná autorita) s technikou překonávání věkového rozdílu mezi obětí a útočníkem. V rámci komunikace hromadně oslovoval vyhlédnuté ženy, mezi kterými si vybíral oběti ochotné dorazit na osobní schůzku. Útok na oběť byl jednorázový, ale razantní – během první schůzky došlo ke znásilnění a vraždě.

Případy kybergroomingu (Česká republika)

Případ „Piškot a Meluzín" (2013)

Dva homosexuálně orientovaní vedoucí Junáku Martin Mertl (22 let) alias Piškot a Milan Machát (20 let) alias Meluzín pomocí propracovaných technik manipulace zneužili v průběhu několika let 39 dětí (36 chlapců a 3 dívky) ve věku od 12 do 18 let. V listopadu 2013 byli odsouzeni ke dvěma desetiletým trestům odnětí svobody. Podle soudu se dopustili znásilnění, sexuálního nátlaku, ohrožování výchovy dítěte, výroby dětské pornografie a dalších skutků

V rámci procesu manipulace dětí využívali zejména falešných profilů dívek, skrz které komunikovali s nezletilými chlapci. Pomocí fiktivního profilu dívky na sociální sítí Facebook např. oslovili 12letého heterosexuálního chlapce, který chodil do oddílu, jenž vedli. Chlapci psali, jak se jim líbí, a postupně si s ním vytvořili virtuální vztah. Chlapec se po čase chtěl s „dívkou sejít", ta po něm však požadovala tzv. důkazy lásky (14).

První důkaz lásky představovala fotografie obnaženého chlapce. „Dívka" chlapce pochválila, ocenila jeho fotografii, ale požadovala další důkaz lásky – fotografii či video, na kterém bude zachycen při sexu s mužem. To chlapec v první chvíli odmítl. Nicméně na jedné ze schůzek oddílu se svěřil se svým problémem Piškotovi a Meluzínovi, kteří mu nabídli pomoc. Oba vedoucí s chlapcem po schůzkách oddílu provozovali sex, natáčeli se, dávali mu vzniklé materiály a on je nahrával dívce na Facebook. Pokud materiály nechtěl dodat, „dívka" jej vydírala tím, že materiály zveřejní a pošle všem kamarádům a spolužákům. Ze strachu chlapec útočníky poslouchal na slovo.

Použitá strategie útoku

Pachatelé využívali techniku falešné identity (falešný profil dítěte opačného pohlaví) s velmi účinnou technikou vydírání. Pachatelé využívali své autority, vzájemně se ve svém jednání podporovali. Dětské oběti byly zneužívány 4 roky.

Doporučení

Základní způsob, jak účinně bojovat s kybergroomingem a nebezpečnými formami komunikace v prostředí internetu, představuje všeobecná primární prevence a výuka dětí v oblasti bezpečného používání internetových služeb (zejména sociálních sítí). V současnosti v České republice existuje celá řada projektů, které se právě na toto téma zaměřují (např. projekty E-Bezpečí, Seznam se bezpečně!, Webrangers a další). Ministerstvo školství, mládeže a tělovýchovy ČR rovněž tyto preventivní aktivity podporuje v rámci grantového programu prevence rizikového chování.

Kromě dětí je však velmi důležité informovat o rizikových formách komunikace zejména rodiče, ti totiž přestavují ústřední a nejdůležitější článek prevence a jsou schopni působit na děti již v útlém věku.

Literatura

1. Berson IH. (2003) Grooming Cybervictims: The Psychosocial Effects of Online Exploitation for Youth. University of South Florida. USA. Retrieved from http://www.cs.auckland.ac.nz/~john/NetSafe/I.Berson.pdf.

2. Craven S, Brown S, Gilchrist E. Sexual grooming of children: Review of literature and theoretical considerations. Journal of Sexual Aggression. 2006; 12(3): ISSN 1355–2600.

3. Kopecký K, Szotkowski R, Krejčí V. (2014) Risks of Internet Communication IV. Olomouc: Palacky University Olomouc. ISBN 978-80-244-4105-4.

4. The Child Exploitation and Online Protection Centre (2008) CEOP Strategic Overview, Retrieved from: https://www.ceop.police.uk/.

5. Kopecký K, Szotkowski R, Krejčí V. (2013) Nebezpečí internetové komunikace IV. Olomouc: Palacky University Olomouc. ISBN 978-80-244-3087-4.

6. Kopecký K. (2010). Kybergrooming – nebezpečí kyberprostoru. Olomouc: Net University. Retrieved from http://e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5%3Akybergrooming-studie.

7. Choo KR. (2009) Online child grooming: a literature review on the minuse of social networking sites for grooming childlren for sexual offences. Australia Institute of Criminology.

8. Bartoněk J. (2012) Dětská prostituce. Internetový portál E-Bezpečí. Olomouc: Univerzita Palackého. Retrieved from http://www.e-bezpeci.cz/index.php/temata/sexting/482--dtska-prostituce.

9. Kopecký K. (2010). Kybergrooming – nebezpečí kyberprostoru. Olomouc: Net University. Retrieved from http://e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5%3Akybergrooming-studie.

10. Kožíšek M. (2014) Aktuální trendy v sociálním inženýrství. Praha: Seznam.cz.

11. Kožíšek M. (2015) Rizika sociálních sítí. Praha: Seznam.cz.

12. Kopecký K. (2014) Stručný úvod do problematiky online vydírání českých dětí se zaměřením na tzv. sextortion. In Pediatrie pro praxi. Olomouc: Solen Medical Education, Vol. 15/6. ISSN 1213–049.

13. Kopecký K, Kožíšek M. (2013) Falešné webkamery jako prostředky získávání intimních materiálů. Olomouc: Univerzita Palackého (prezentace).

14. Kopecký K, Szotkowski R, Krejčí V. (2014) Risks of Internet Communication IV. Olomouc: Palacky University Olomouc. ISBN 978-80-244-4105-4.

15. Vnouček P. (2010) Facebookový vrah má doživotí. Sociální síť sklízí kritiku. In: Týden.cz [online]. Retrieved from: http://www.tyden.cz/rubriky/media/ internet/facebookovy-vrah--ma-dozivoti-socialni-sit-sklizi-kritiku_161662.html.

16. Carter H. (2010) Merseyside police refers itself to IPCC over Facebook killer Peter Chapman. In: Guardian. Retrieved from http://www.guardian.co.uk/uk/2010/mar/09/merseyside-police-peter-chapman-facebook.

17. GUY P. (2009) Facebook suspect's ex: He 'killed my double'. In: The Sun [online]. Retrieved from: http://www.thesun.co.uk/sol/homepage/news/2704262/ Facebook-suspect--killed-my-double.html.

18. Stokes P. (2010) Peter Chapman targeted thousands of young girls. In: Telegraph [online]. 2010 Retrieved from: http://www.telegraph.co.uk/news/ uknews/crime/7397894/Peter--Chapman-targeted-thousands-of-young-girls.html.

Článok je prevzatý z
Pediatr. praxi 2015; 16(5): 331–333

Mgr. Kamil Kopecký, Ph.D.
Centrum prevence rizikové virtuální komunikace,
Pedagogická fakulta UP v Olomouci
Žižkovo nám. 5, 771 40 Olomouc
kamil.kopecky@upol.cz