Stručný úvod do problematiky online vydírání českých dětí se zaměřením na tzv. sextortion

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

Online vydírání dětí v prostředí internetových služeb (sociálních sítí) se stalo velmi nebezpečným fenoménem, který v českém prostředí v pozici oběti zažilo 6–8 % dětí. Většina závažných případů vydírání postupuje podle několika základních schémat, podle kterých lze rozpoznat, že je virtuální komunikace riziková. Na základě podrobné analýzy 15 případů online vydírání autor vytvořil model, podle kterého internetoví útočníci v praxi postupují. Model je pro zpřehlednění rozložen do několika vzájemně propojených fází, kterými online útok postupuje. Jednotlivé fáze jsou rozvedeny s použitím autentického důkazního materiálu.

Klíčová slova: online vydírání dětí, kyberšikana, model online vydírání, fáze vydírání, sdílení intimních materiálů, sexting.

A brief introduction to the issue of online blackmail of Czech children with a focus on sextortion

The online extortion and/or sextortion of children is a dangerous phenomenon related to the use of internet services (social networks, etc.). There is, as estimated, about 6–8% of the child population in the Czech Republic affected by it. In the majority of serious cases of extortion the process evolves through an elementary succession of communication advances that makes it possible to recognize the ongoing interchange as dangerous. On the basis of a detailed analysis of 15 serious cases of online extortion, a model has been developed, according to which the internet offenders proceed in their practice. The model is, for clarity sake, divided into several mutually interconnected stages, through which the attack proceeds. The individual stages are elaborated on, using authentic evidence.

Key words: sextortion, extortion, humiliation, child abuse, model of sextortion, phases of exortion, sexting, cybergrooming.

Pediatr. praxi 2014; 15(6): 352–354

Vydírání dětí v prostředí internetu

Vydírání dětí v prostředí internetu se stalo do jisté míry tabuizované téma. Je to dáno na jedné straně povahou materiálů, které jsou k vydírání využity, na straně druhé snahou neupozornit na jednotlivé případy s cílem neuškodit obětem, případně případy vydírání ututlat a pokusit se je řešit jinak (např. bez policejní intervence).

Počet případů dětí vydíraných v prostředí internetu roste jak v Evropě, tak i ve Spojených státech a Kanadě. Podobný vývoj lze sledovat také v České republice. Opřeme-li se o aktuální data, podle výzkumu Nebezpečí internetové komunikace IV (etapa 2012–2013) realizovaného týmem projektu E-Bezpečí Univerzity Palackého v Olomouci a společnosti Seznam.cz na vzorku více než 21 000 dětí zažilo vydírání v pozici oběti 7,33 % českých pubescentů (1). Dle zjištění obou organizací pak většina závažných případů vydírání dětí postupuje podle jednoduchých, ale velmi nebezpečných schémat, na která se zaměříme v dalších částech textu.

Následující text vznikl na základě analýzy 15 případů vydírání dětí evidovaných a řešených Online poradnou projektu E-Bezpečí (www.napisnam.cz). Analýza případů vydírání dětí probíhala od 1. 1. 2012 do 30. 5. 2014.

Ve všech případech vydírání probíhalo prostřednictvím internetových služeb, zejména v prostředí sociálních sítí (Facebook, ASK.fm aj.). V téměř ¾ případů (11/15) se obětí vydírání stala dívka, v přibližně ¼ chlapec. Věk obětí se pohyboval v intervalu 11–17 let. V průběhu řešení případů členové výzkumného týmu monitorovali synchronní i asynchronní komunikaci oběti a útočníka, zapojili se do profilování pachatele a do sledování aktivit pachatele v rámci dalších internetových služeb. Ve všech sledovaných případech byla skutečná identita pachatelů odhalena. Časový interval vydírání analyzovaných případů se pohyboval v rozmezí 2 týdny až 3 měsíce. Ve všech případech byla pachatelem dospělá osoba (věk 28–39 let).

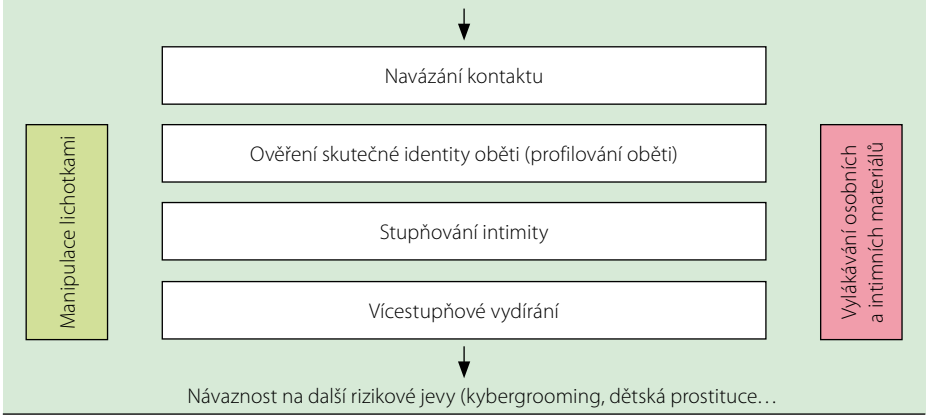
Modely chování pachatelů

Výsledkem analýz je zjištění, že se pro vydírání dětí využívá celá řada velmi podobných technik, které jsou zaměřeny na vzbuzení důvěry, vylákání intimního materiálu a následné vydírání. Většina z analyzovaných případů rovněž probíhá podle velmi podobných schémat a postupů. Na základě analýz jsme vytvořili model vydírání, rozdělený do logických postupně navazujících fází. Model si vysvětlíme podrobněji.

1. fáze – navázání kontaktu s dítětem

V této fázi útočník navazuje kontakt s dítětem, který obvykle zahajuje jednoduchou větou: *Ahoj, vyměníme si fotky? Ahoj, pokecáme? Ahoj, jak*

Obrázek 1. Model vydírání dítěte s využitím ICT (prostředí sociálních sítí)



se vede? Útočník zpravidla vystupuje pod identitou osoby stejného pohlaví, jako je oběť, tedy dívka píše dívce, chlapec píše chlapci. V případě, že by dívka psala chlapci, pravděpodobně již nepůjde pouze o vydírání, ale také o tzv. kybergrooming – tedy vydírání postupně přejde k lákání na osobní schůzku s obětí.

Pokud dítě na podnět ke kontaktu pozitivně zareaguje *(Dobře, vyměníme si fotky. JJ.)*, útočník pravděpodobně dítěti pošle první fotografii či přímo „sérii" fotografií, které zpočátku nejsou zaměřeny intimně. Intimita nastupuje až v dalších etapách.

V několika případech také pachatel vyhlédnutou oběť kontaktoval jakoby náhodně, omylem.

Ahoj, promiň, něco jsem na internetu hledala a omylem jsem si tě přidala do přátel. Já jsem Pavla. Můžeme si spolu třeba psát, chceš?

Postupně pak přesvědčil dítě, aby s ním začalo komunikovat a poskytlo mu informace osobního, a zejména intimního charakteru (2).

2. fáze – manipulace lichotkami

Aby útočník získal zájem a pozornost dítěte, začne všechny materiály, které mu oběť zaslala, velmi pozitivně hodnotit. Tj. jakmile mu oběť zašle fotografii, začne jí útočník lichotit a fotografii komentuje např. takto: *Ty jsi na té fotce nádherná. Máš krásné tělo. Moc ti to sluší. Jsi překrásná. Lichotku pak obvykle doplní o větu: Pošleš mi další?* Touto metodou si dítě poměrně snadno získá – děti touží po obdivu a uznání, chtějí, aby je někdo obdivoval a ocenil. Manipulace lichotkami plynule prostupuje všemi následujícími fázemi.

3. fáze – ověření skutečné identity oběti

V této fázi se útočník snaží potvrdit identitu oběti. To dělá tak, že např. po dítěti požaduje, aby se mu vyfotilo s konkrétním nápisem a datem (např. *Pro Janičku, 31. 5. 2013*). Útočníkovi v této fázi vydírání nejde o to, aby získal fotografii obličeje či intimní fotografii dítě, ale pouze si ověřil, jestli s konkrétním dítětem skutečně komunikuje a zda jsou fotografie opravdu autentické.

Ověřování identity útočník zpravidla uvozuje větou: *Ne, na té fotce nejsi ty. Nevěřím. Normálně se mi vyfoť třeba mobilem a napiš k tomu Pro Terezku. Jo ale nemusí ti tam být vidět obličej…*

Technika identifikace osob na internetu pomocí fotografií s konkrétním nápisem, datem nebo např. aktuálními papírovými novinami se běžně využívá k potvrzování identit osob na internetu. Sama o sobě je tak veskrze pozitivní, přesto ji lze zneužít právě v rámci vydírání.

4. fáze – stupňování intimity

Tuto fázi jsme nazvali stupňování intimity, protože intimita fotografií, které si navzájem oběť s útočníkem vyměňují, se zvyšuje a stupňuje. Fotografie zachycující nejdříve oblečené dítě postupně nahrazují fotografie, na kterých je dítě částečně či úplně svlečené, až k fotografiím, na kterých si 12leté děti do análního či vaginálního otvoru zasouvají prsty apod. Obdobné fotografie pak samozřejmě útočník dítěti rovněž zasílá, obvykle se jedná o fotografie ze zahraničních erotických či pornografických portálů. Většina materiálů zasílaných oběti útočníkem spadá do oblasti dětské pornografie. Fáze stupňování intimity je velmi nebezpečná, protože dítě napodobuje chování útočníka a je schopno zaslat mu téměř cokoli.

Aby útočník překonal stud dítěte, zpravidla mu nejdříve nabídne vlastní intimní fotografie, které jsou samozřejmě podvrhy (fotografie získané z veřejných či privátních fotogalerií) a není na nich zachycen útočník. Dítě poté začne vnímat distribuci intimních materiálů jako něco běžného a přirozeného a útočníkovi poté poskytne svoje vlastní záběry.

5. fáze – vícestupňové vydírání

Pokud se dítě rozhodne opustit schéma výměny fotografií, útočník zpravidla přejde k vydírání. To je realizováno obvykle dvěma způsoby:

a) *vydíráním prostřednictvím „přátel" na sociálních sítích,*
b) *vydíráním prostřednictvím rodičů oběti.*

V etapě vydírání prostřednictvím přátel na sociálních sítích útočník vyhrožuje dítěti, že pokud mu nepošle další materiály, rozešle vše, co od něj/ní získal přátelům oběti a dalším uživatelům sociálních sítí, takže rychlost šíření těchto materiálů bude velmi vysoká. Útočník volí například tyto formulace: *Rozešlu to všem, co mám v přátelích a které mám v odběrech. Takže se mi ještě párkrát vyfotíš a pošleš mi to, jak budu chtít, nebo to dám na internet a všichni tvoji kamarádi to uvidí a bude trapas. Je ti to jasný? Takže to všechno hezky pošli* (ukázka komunikace ze skutečného případu).

Na dalším stupni vydírání se forma útoku opakuje s tím, že je k vydírání využit rodič oběti. Pravděpodobnost, že útočník postupně získá další intimní materiály od dítěte, roste. V řadě případů pak pachatel dítě s využitím intimních materiálů donutí k osobní schůzce. Vydírání dále může přerůst až v prostituční chování, protože řada abuzérů na osobních schůzkách nabízí dětem peníze za poskytnutí sexuální služby. Děti se pak za pachatelem dobrovolně vracejí.

100 % obětí v průběhu vydírání nekontaktovalo žádnou dospělou osobu (rodiče, učitele, dospělé sourozence), v pokročilých etapách vydírání děti kontaktovaly anonymní internetovou poradenskou linku. Ta poté začala s dítětem komunikovat a kontaktovala Policii ČR k dalšímu šetření. Z toho lze předpokládat, že velké množství případů není policii vůbec nehlášeno a nefiguruje tak v oficiálních statistikách internetové kriminality.

Jak jsme demonstrovali na konkrétních příkladech, online vydírání je v řadě případů schematické. V chování pachatelů lze vysledovat urči-

Obrázek 2. Ukázka navázání kontaktu s dítětem v prostředí Facebooku (skutečný případ a jméno fiktivní)

Obrázek 3. Útočník (Monika) zasílá dítěti podvrženou galerii intimních fotografií

tě opakující se formy komunikace, ze kterých lze odvodit další vývoj samotného procesu vydírání.

Literatura

1. Kopecký K, Szotkowski R, Krejčí V. Risks of Internet Communication IV. Olomouc: Palacky University Olomouc, 2014.
2. Kopecký K. Riziková forma navazování kontaktů s dětmi v prostředí sociálních sítí. E-Bezpečí. Olomouc: Univerzita Palackého, 2014.

Další doporučené zdroje

1. Beck L. Anonymous Outs the Man Who Allegedly Drove Amanda Todd to Suicide. Jezebel.com. Dostupné z http://jezebel.com/5952080/anonymous-names-names-outing-the-man-who-allegedly-drove-amanda-todd-to-suicide.
2. Blankstein A. FBI arrests suspect in Miss Teen USA 'sextortion' case. NBC News. Dostupné z http://www.nbcnews.com/news/other/fbi-arrests-suspect-miss-teen-usa-sextortion-case-f8C11267183.
3. Grosskopf A. Online interactions involving suspected paedophiles who engage male children, Trends and Issues in Crime and Criminal Justice No. 403, Australian Institute of Criminology. Dostupné z http://www.aic.gov.au/documents/C/8/C/%7BC8C25B82-6F4A-4119-BC62-75840BA8D22A%7Dtandi403.pdf.
4. Kloess JA, Beech AR, Harkins L. Online Child Sexual Exploitation: Prevalence, Process and Offender Characteristics. Trauma, Violence & Abuse 2014; 15(2): 126–139.
5. Mitchell KJ, Finkelhor D, Wolak J. The Internet and family and acquaintance sexual abuse. Child Maltreatment, 2005; 10: 49–60. doi: 10.1177/1077559504271917.
6. O'Connell R. A Typology of Cybersexploitation and On-line Grooming Practices. s. Dostupné z http://www.jisc.ac.uk/uploaded_documents/lis_PaperJPrice.pdf.
7. Strasburger VC. Children, Adolescents, and the Media. Pediatric Clinic of North America, 2012; 59(3). Dostupné z http://adolescenciasema.org/usuario/documentos/Health%20Effects%20of%20Media%20PCNA%202012.pdf.
8. Wilson C. Feds: online "sextortion" of teens on the rise. Associated Press, 2010. Dostupné z http://www.msnbc.msn.com/id/3871425 9/ns/technology_and_science-security/t/feds-online-sextortion-teens-rise/. Accessed August 22, 2011.

Článek doručen redakci: 25. 6. 2014
Článek přijat k publikaci: 11. 7. 2014

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