Příručka Kybergrooming

Termín kybergrooming označuje postupy uživatelů internetových komunikačních médií (chat, ICQ apod.), kteří se snaží získat důvěru dítěte s úmyslem ho zneužít (hlavně sexuálně) nebo vést k nelegálním aktivitám. Kybergrooming představuje psychologickou manipulaci oběti spojenou se sexuálním násilím. Kybergroomer je dospělá osoba, většinou muž, ale může to být i žena, která komunikuje s dítětem přes digitální technologie v naději, že získá odhalující materiály nebo je přesvědčí k osobnímu setkání. Sexuální predátoři, kteří vylákají oběť do reálného světa a zneužijí ji, jsou v menšině. Většina útočníků se uspokojuje s on-line vztahem, komunikují s dítětem přes videohovor, kde je nutí se odhalovat či zasílat intimní materiály.

Kybergroomeři jsou často mylně považováni veřejností za pedofily. Pedofilie je však vzácná sexuální deviace. Většina internetových sexuálních predátorů by upřednostňovala dospělé partnery, ale kvůli dětské nezkušenosti, zvědavosti a snadné manipulaci si volí tito predátoři za své oběti právě děti. Neplatí vždy obvyklé představy zoufalých a osamělých mužů, kteří se tímto způsobem uspokojují sexuálně. Určitě jich na internetu najdeme mnoho, ale velká část predátorů jsou také mladí a zdánlivě nevinní muži nebo úspěšní a vzdělaní jedinci s vlastními rodinami a dětmi.

Ohrožení kybergroomingem mohou být jak mladiství, tak i nejmladší děti. Větší riziko hrozí těm, kteří tráví na internetu hodně času, nejsou obezřetní ve vytváření on-line přátelství, jsou v období života, kdy pociťují silný zájem o sex a partnerské vztahy, jsou otevření novým zážitkům a riskantním situacím, trpí nedostatkem sebevědomí, lásky a pozornosti ze strany rodičů nebo si nedovedou přiměřeně neuvědomit možné následky takového jednání. Někteří experti tvrdí, že jsou ohroženější dívky, jiní zdůrazňují zranitelnost chlapců, o které mají predátoři také velký zájem. Z mých osobních zkušeností je patrné, že chlapci jsou stejně ohrožení jako dívky.

Průběh útoku

1) Příprava na kontakt s dítětem: V této fázi připravuje útočník svou falešnou identitu, kterou později použije k oslovení dítěte. Falešný profil upraví tak, aby co nejlépe zapadal do světa oběti či do okruhu svého zájmu. Pokud cílí na mladé dívky, vydává se za mladého a atraktivního chlapce či dívku stejného věku, se kterou by se oběť mohla chtít skamarádit. V případě zájmu o chlapce, zvolí postup s opačnými rolemi a podobně. Mimo pohlaví, věku a vzhledu přizpůsobí podle oběti i zájmy a koníčky, vytváří tak novou identitu, za kterou se může skrýt. Falešné fotografie může stáhnout z internetu nebo použít materiály od svých předešlých obětí.

Různí sexuální predátoři používají různé strategie. Někteří mají k dispozici jeden či více falešných profilů, které pečlivě upravují a zdokonalují, aby působily co nejvíce autenticky. Ukrytí za těmito profily následně oslovují své oběti, někdy dokonce hromadně kontaktují několik dětí současně, za účelem zvýšit své šance na úspěch. V situaci, kdy má útočník více falešných identit, je může využít k přesvědčování dítěte o své důvěryhodnosti tím, že ostatní své falešné profily představuje jako své skutečné přátele z reálného života, kteří mohou potvrdit jeho existenci a tvrzení. V pozadí však stojí pouze jeden predátor. Útočník může také vytvořit dynamický profil, který upravuje podle informací získaných o své současné oběti. Jedná se o mnohem cílenější útok, kdy predátor zkoumá chování, zájmy a okolí oběti na základě nichž vytváří profil. Dítě pak má pocit, že jsou si podobní, že mají stejné zájmy a rozumí si. Tím se zvyšuje pravděpodobnost toho, že se dítě otevře a predátor dosáhne svého cíle.

Někteří pachatelé využívají metodu falešné autority, kdy se vydávají za zaměstnance společnosti, která dětem nabízí atraktivní příležitosti, jako jsou soutěže, finanční pomoc, dárky, možnosti kariéry a podobně. Útočník zveřejní inzerát a čeká, až se oběti samy ozvou. Autorita společnosti zaručuje důvěryhodnost. Nakonec získá útočník důležité osobní údaje dítěte, jako jsou telefonní číslo, adresa bydliště, adresa školy, fotografie a další.

2) Kontaktování dítěte, budování vztahu: Když má predátor připravenou svou falešnou identitu, oslovuje dítě prostřednictvím internetu. Manipuluje oběť například skrze zrcadlení - snaží se imitovat děti, tvrdí, že sdílí podobné zájmy, postoje a problémy. Projevuje toleranci, přátelství, empatii a poskytuje oběti podporu. Nešetří lichotkami a může i věnovat dárky s úmyslem získat důvěru a vytvořit vazbu. Jeho cílem je rovněž získat co nejvíce osobních informací a zjistit, do jaké míry rodiče monitorují dítě online. Predátor nesmí riskovat odhalení, proto zjišťuje, kde má dítě počítač, zda je samo doma a snaží se ho odradit od sdílení jejich konverzace s rodiči.

3) Získání intimních materiálů: Po nějaké době začne predátor do konverzace postupně zapojovat téma sexuality, zjišťuje vztah dítěte k jeho vlastní sexualitě, zajímá se o jeho zkušenosti, začne vyžadovat vzájemné posílání intimních materiálů nebo odhalování před kamerou. Tyto materiály následně použije k vydírání dítěte a dále žádá další, odhalenější materiály nebo osobní schůzku.

4) Osobní setkání: Toto setkání nemusí být cílem každého kybergroomera, ale existuje skupina jednotlivců, kteří se snaží navázat osobní kontakt s dítětem. Důsledky mohou být katastrofální. Předtím, než dojde k osobnímu setkání nebo na jeho počátku, bývá nutné překonat věkový rozdíl, protože dítě má dojem, že útočník je stejně starý. Tito predátoři tvrdí, že jsou rodiče nebo příbuzní online kamaráda dítěte, zatímco někteří postupně navyšují svůj věk ještě před osobní schůzkou.

Kybergroomeři vykazují velkou trpělivost a celý tento proces může trvat několik měsíců. Dítě se může dokonce zamilovat do predátora a vytvořit si k němu hluboký vztah. Nemusí to tak ale být vždy. Někdy to může naopak trvat jen několik dní nebo dokonce hodin, během nichž útočník naváže kontakt s obětí a získá od ní nebezpečný materiál.

Dopady na oběť

Kybergrooming jeví značné negativní dopady na dětské oběti. Tyto důsledky jsou značně závažné a mohou trvale ovlivnit fyzické, emocionální a psychické zdraví dítěte. Prvním zjevným dopadem je psychické trauma, které může vést ke stresu, úzkostem, depresi, nízkému sebevědomí, a dokonce i k sebevražedným myšlenkám. Dítě se může cítit výrazně ohrožené a strachovat se, že kybergroomer rozešle jeho intimní materiály mezi rodinu a přátele dítěte, což ovlivňuje jeho každodenní život a normální fungování.

Kybergrooming může také zapříčinit izolaci dítěte od rodiny, přátel a okolí, vůči kterým může cítit silný stud. Pokud mělo dítě ke kybergroomerovi silný vztah, může pociťovat smutek ze ztráty blízkého člověka, a to i přesto, že šlo o falešný profil. V neposlední řadě může kybergrooming způsobit problémy v akademickém životě, sníženou školní úspěšnost a odtažitost od vzdělávacího procesu.

Webcam trolling

Pokud se bavíme o online seznamování, je důležité děti seznámit s možnostmi ověření identity. Jednou možností, jak si ověřit, že za profilem je opravdu ten, za koho se uživatel vydává, je požádat druhou stranu o fotografii s obličejem, na které drží nějaký specifický předmět (např. papír s dnešním datem a větou, kterou mu nadiktujeme).

Je však důležité, aby nám druhá strana fotografii zaslala během následujících pěti minut, aby případný podvodník neměl možnost fotografii upravit či zfalšovat. Jakékoli výmluvy jsou výstrahou a znakem, že na druhé straně by se mohl nacházet predátor.

Dalším způsobem, jak si prověřit identitu je za pomocí videohovoru. U tohoto způsobu však musíme dávat pozor na tzv. Webcam trolling. Jedná se o taktiku, kdy predátor pomocí speciálního programu pouští do kamery předem připravenou videosmyčku (kterou mohl například stáhnout z internetu) a oběti tvrdí, že mu nefunguje mikrofon, ale aspoň se můžou vidět a můžou si psát přes chat.

Webcam trolling může být rozeznatelný například podle neadekvátních reakcí druhé strany, ale také člověku nemusí být patrný. Kvůli této taktice nepovažujeme videohovor bez funkčního mikrofonu za spolehlivé ověření identity.

Použité zdroje

KOSOVÁ, Lucie a MARTINEK, Petr. Bezpečně v kyber!. Online. Národní úřad pro kybernetickou a informační bezpečnost. 2020. Dostupné z: https://www.nukib.cz/download/publikace/vzdelavani/Brozura%20bezpecne%20v%20cyber_A5.pdf.

MAŠKOVÁ, Anna; LUKÁŠOVÁ, Kateřina; PACÁK, Rastislav a BRANDEJSOVÁ, Jana. KYBERGROOMING A KYBERSTALKING - Metodický materiál pro pedagogické pracovníky. Online. Národní centrum bezpečnějšího internetu. 2012. Dostupné z: https://www.ncbi.cz/odborna-knihovna/category/6-metodiky-ucebni-materialy.html?download=37:metodika-kybergrooming-a-kyberstalking.

KRČMÁŘOVÁ, Barbora; VACKOVÁ, Kristýna; HÝBNEROVÁ, Jana; HULANOVÁ VELIČKOVÁ, Lenka; LANGROVÁ, Aneta et al. Děti a online rizika - sborník studií. Online. Praha: Sdružení Linka bezpečí, 2012. ISBN 978-80- 904920-3-5. Dostupné z: http://www.vyzkum-mladez.cz/zprava/1378730032.pdf.

SZOTKOWSKI, René; KOPECKÝ, Kamil a KREJČÍ, Veronika. Nebezpečí internetové komunikace IV. Online. Olomouc: Univerzita Palackého v Olomouci, 2013. ISBN 978-80-244-3911-2. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/58-nebezpeci-internetove-komunikace-iv-2012-2013/file

KOPECKÝ, Kamil; SZOTKOWSKI, René a DOBEŠOVÁ, Pavla. Riziková komunikace a seznamování českých dětí v kyberprostoru. Online. Křížkovského 8, 771 47 Olomouc: Univerzita Palackého v Olomouci, 2021. ISBN 978-80-244-5914-1. Dostupné z: https://doi.org/10.5507/pdf.21.24459141.

Licence