E-Bezpečí 2020, 5(1): Page 80-85. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=1839

MARTIN KOŽÍŠEK: ZÁKLADEM ÚČINNÉ PREVENCE JE VYBUDOVÁNÍ DŮVĚRNÉHO VZTAHU S DÍTĚTEM. RESTRIKCE JSOU MÁLO EFEKTIVNÍ.

Kamil KOPECKÝ

Stál u zrodu sociální sítě Lidé.cz, kterou také řadu let spravoval jako její admin. Zásadním způsobem v ČR rozjel preventivní projekt Seznam se bezpečně, pod jeho vedením vznikla celá řada preventivních videí orientovaných na online seznamování a s ním související rizika, které školy používají dodnes. Nakonec zakotvil v CZ.NIC, kde převzal roli koordinátora projektu Safer Internet v ČR. Dnešní rozhovor povedeme s Martinem Kožíškem.

V oblasti online bezpečnosti se pohybujete bezmála 15 let. Zkuste nám stručně popsat vaši profesní cestu od Lidé.cz k CZ.NIC a programu Safer Internet.

Tři roky po založení Seznamu jsem brouzdal v internetové kavárně a našel jsem inzerát hledající brigádníka. Za dva dny si mě pozval Ivo Lukačovič a udělal se mnou přijímací pohovor. Měl jsem štěstí, že jsem stál po boku mnoha nadšenců a byl u zrodu mnoha zajímavých služeb. Několik z nich (Lidé.cz, Spolužáci.cz) jsem pak dále rozvíjel. K tomu co nyní dělám, mě přivedla nešťastná událost, která se stala na Lidé.cz. Na začátku byl příběh mladé dívky, která spáchala sebevraždu z důvodu úniku intimních fotek na internet.

Vznikl tak projekt Seznam se bezpečně, který fungoval deset let. Po jeho skončení jsem se rozhodl pokračovat ve sdružení CZ.NIC. To hlavní co mě přesvědčilo bylo, že tyto projekty CZ.NIC nedělá jen kvůli svému CSR. Což byl i důvod, proč jsem odmítl několik komerčních firem. Vést národní Safer internet centrum je velká výzva s možností hodně věcí změnit na národní úrovni.

(Martin Kožíšek)

Jako profesionál se pohybujete

především v prostředí sociálních sítí. V čem spatřujete jejich největší pozitiva? A jaká podle vás představují rizika?

Díky sociálním sítím se jednodušeji propojujeme s ostatními lidmi, dostáváme se rychleji k informacím i obsahu a má to celou řadu pozitiv. Na druhou stranu tím otvíráme zadní vrátka ke svému soukromí, která může někdo zneužít. Velká část rizik jde za samotnými uživateli, kteří služby zneužívají. Druhou část pak mají na svědomí samotné služby. Ve snaze nás na síti co nejdéle udržet, nám doporučují obsah, přátele, témata nebo nám jen řadí obsah. Tyto algoritmy nás uzavírají do sociálních bublin, kde slyšíme jen echa vlastních názorů. Paradoxně místo propojování s ostatními dochází k rozdělování společnosti nebo radikalizaci.

Vstup do sociálních sítí je často limitován věkem (v ČR od roku 2019 nově od 15 let). Má tento limitovaný přístup k online službám skutečně smysl? Zastaví dítě?

Nejotravnější na celém internetu je povinnost neustále něco odklikávat, že s něčím souhlasím nebo jsem byl srozuměn. Tyto disclaimery jsou na službách jen proto, aby se ochránil provozovatel, nikoli uživatelé. Neznám žádného dospívajícího, kterého by informace, že je služba až od 18 let odradila a rozmyslí si návštěvu. U sociálních sítí je to obdobně. Děti falšují věk, často s vědomím rodičů. Tudy cesta nevede.

Ve své práci jste se setkával s různými druhy pachatelů sexuálně motivované trestné činnosti, zjednodušeně tzv. online predátory. Dokázal byste stručně charakterizovat typického pachatele?

Čím je specifický? Jak se chová?

Internetoví sexuální útočníci nepřišli s nástupem sociálních sítí typu Facebook, měli jsme je na našich sítích dávno předtím. Co můžeme pozorovat, jsou stále stejné postupy při zneužívání dětí. Těch základních vzorců je zhruba sedm. Za těch 25 let se změnily pouze použité technologie, je rychlejší internet, můžeme sdílet fotografie, videa nebo využívat aplikace. Nejčetnější skupinou, která umí zdatně zmanipulovat dítě na sociální síti, jsou lidé ve věku 17-26 let. Tím ale neříkám, že dítě nemůže zneužít někdo starší.

Dá se nějakým způsobem charakterizovat i typická dětská oběť?

Nejzranitelnější skupinou jsou děti ve věku 11-17 let. Pachatelé také preferují určitý typ vzhledu, lákají je daleko více děti, které jsou blonďaté apod. Paradoxně nejsou mezi nejčastějšími oběťmi děti ze sociálně slabšího prostředí. Přibývá obětí z řad dětí, které mají množství koníčků, sportují a k internetu či technologiím se pak dostávají méně často. To může být značný handicap vůči různým internetovým útočníkům.

Co by měl rodič udělat v situaci, kdy zjistí, že se jeho dítě stalo terčem online útoku - např. vydírání či vyhrožování? Je žádoucí např. zablokovat komunikaci s pachatelem? A kdy se obrátit na policii?

Rodič by měl tuto situaci co nejdříve nahlásit policii, ideálně s nějakými důkazy, záznamem komunikace apod. Rozhodně by neměl v komunikaci pokračovat, manipulovat s ní, případně mazat či jinak blokovat kontakt.

Ve své práci se samozřejmě věnujete prevenci. Na jaká témata by se v

souvislosti s online bezpečností měli zaměřit rodiče, jejichž děti začínají aktivně využívat internetové služby?

„Nových dětí“ si na internetové službě díky algoritmu sítě může všimnout kdokoli. Díky němu je vyšší šance, že bude osloveno neznámými lidmi. Proto bych dětem vysvětlil pravidla sdílení obsahu, informací a navazování nových přátelství nebo bezpečné komunikace. Děti by se měly naučit možnosti ověřování profilu a také to, jak se bránit a kde se mohou obrátit o pomoc .

Měli by rodiče dětem regulovat, k jakému obsahu se dítě prostřednictvím počítače, mobilního telefonu či tabletu dostane?

Nejsem zastánce nějakých zákazů. Navíc v období dospívání ztrácejí veškeré zákazy a omezení smysl. Děti jsou technologicky napřed a dokáží celou řadu nastavení jednoduše obejít. Kontrolovat obsah nebo používat rodičovské zámky má smysl jen u malých dětí. U starších dětí je lepší s nimi budovat důvěru.

Co by měl dělat rodič, na kterého se např. obrátí desetileté dítě s tím, že chce mít účet na sociální sítí? Jak reagovat?

Za sociální síť se dá dnes považovat i Youtube nebo WhatsApp. Současné věkové nařízení pro využívání sociálních sítí od 15 let je nesmysl. Rodič si ale může nastavit pravidla, že určitou službu dítěti povolí, ale bude k ní mít přístup.

(Martin Kožíšek hledí vstříc dalším výzvám. Foto: iDnes.cz)

Když se odkloníme od tématu dětí a sexuálně motivovaných trestných činů, k dalším druhům kyberkriminality patří také různé druhy online podvodů. Setkal jste se s nějakými případy podvodného jednání, ve kterých např. došlo k finančním ztrátám apod? Na co by si měli dávat pozor dospělí uživatelé, kteří chtějí v online světě např. nakupovat či prodávat?

Podvodů je celá řada. Od sofistikovaných phishingových až po zcela banální, kdy ze mě bude chtít někdo vymámit heslo. Na jedné straně se někdo může dostat jen k informacím, ale také může jít o podvody, ve kterých mohou lidé přijít o peníze. Nejčastěji se lidé nechávají „nachytat“ na nízkou cenu. Ve snaze ušetřit jsou ochotni riskovat nákup přes neověřené e-shopy, bazary nebo od neznámých lidí. Doporučil bych využívat srovnávače ověřených

obchodů a vyvarovat se nákupům s posílání záloh. Důležité je to, že pokud budu podveden a to třeba i o banální částku, měl bych vše oznámit co nejdříve na policii.

Významným tématem posledních let jsou také dezinformace a fake news, které často v populaci vyvolávají nenávistnou odezvu (hate crime). Zažíváme je pravidelně např. v souvislosti s volbami, v současnosti však také v souvislosti s epidemií COVID-19. Na co si mají uživatelé ve vztahu k dezinformacím dávat pozor? A mají vlastně dezinformace reálný dopad?

Na jedné straně chceme, aby se podobný obsah na internetu nenacházel, na druhé straně jsme citliví na naši svobodu na sítích. Neexistuje jednoduchý způsob pro provozovatele služeb, jak nakládat se závadným obsahem. Část může jít odstranit roboticky (například dětská pornografie nebo jiný závadný obsah), část lze odstranit jen ručně. Některé velké sítě už k odstraňování podobného typu obsahu přistoupily, některé služby zamezily zobrazování reklamy na ně. Jak už jsem zmínil na začátku rozhovoru, za mnohými problémy stojí algoritmy, které nás uzavírají do bublin, kde se dostaneme jen k určitému proudu informací. Dezinformace jsou tu odjakživa, bránit se můžeme třeba i tím, že dáme větší prostor předmětům vztahujícím se k mediální gramotnosti.

V roce 2017 jste se podílel na výzkumu, jehož výstupem byla výzkumná zpráva Starci na netu. V něm uvádíte, že nejaktivnějšími šiřiteli e-mailového

spamu, ať již pravdivého či nepravdivého, jsou senioři ve věku od 65 let. Čím si to vysvětlujete? Jsou mezi těmito seniory jen šiřitelé nebo i tvůrci?

Já na zveřejnění tohoto výzkumu vzpomínám hlavně proto, že jsem nikdy v mé profesní kariéře nedostal během tak krátké doby tolik výhrůžných zpráv smrtí mě a mojí rodině (Poznámka: Podobné reakce si zažili členové týmu E-Bezpečí, spoluautoři výzkumu). Vysloužil jsem si i několik zmínek na dezinformačních webech, kde se objevil můj telefon. Zarazilo mě, že se lidé při výhrůžkách ani nesnažili schovat pod nějakou anonymní identitu. Dokonce mi přišel dopis klasickou poštou se známkou a razítkem se zprávou, že budu viset. Je neuvěřitelné, kolik lidí výsledky tohoto výzkumu zmobilizovalo a mělo čas je tak rychle rozšířit.

Martine, děkujeme a přejeme hodně sil v další preventivní práci!

Rozhovor vedli
Kamil Kopecký, Lukáš Kubala
E-Bezpečí, Univerzita Palackého v Olomouci