E-Bezpečí 2019, 4(1): Page 63-66. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=1470

E-BEZPEČÍ & UPOINT: BESEDA O RIZICÍCH SPOJENÝCH S WEBOVÝMI KAMERAMI UPOZORNILA NA AKTUÁLNÍ HROZBY

Kamil KOPECKÝ

V úterý 19. února 2018 proběhla v prostorách UPointu Univerzity Palackého beseda o rizicích spojených se zneužitím webkamery. Diskutovalo se např. o vyděračském spamu vyhrožujícím zveřejněním intimních materiálů zachycených webkamerou vašeho počítače, o webcam trollingu, útocích prostřednictvím virů, ale také např. o fenoménu sextortion a kybergroomingu. Diskuse se zúčastnili Kamil Kopecký a René Szotkowski z týmu projektu E-Bezpečí Univerzity Palackého v Olomouci a Pavel Schweiner, vrchní komisař oddělení kybernetické kriminality olomoucké policie a odborný konzultant a lektor projektu E-Bezpečí.

Besedu zahájil doc. Kamil Kopecký, který upozornil na novou vlnou **vyděračských e-mailů označovaných jako tzv. virus RAT** (remote access trojan), které straší uživatele e-mailu tím, že neznámý útočník prostřednictvím webové kamery získal přístup k jejich pornografickým materiálům a pokud jim nezaplatí, budou tyto materiály zveřejněny. A jako důkaz obsahoval email přílohu s těmito "materiály". Pokud jste však na přílohu klikli a pokusili se ji stáhnout, mohl být váš počítač infikován právě pomocí viru. Samozřejmě k úniku vašich materiálů nedošlo, smyslem zprávy bylo vystrašit a přimět vás k otevření přílohy. Přesto se však vždy najde dostatek uživatelů, kteří na vyděračský email zareagují a požadovaný obnos vyděrači převedou - během prvních dvou dní šíření na bitcoinovém účtu vyděrače naskočila částka přes 14000

Kč. Policie ČR v této věci vydala i varování, aby uživatelé v žádném případě žádné částky pachateli neplatili. A zároveň upozornila, že není nutné policii nové případy tohoto útoku hlásit, protože je aktivně řeší.

V další části vystoupil dr. René Szotkowski, který upozornil na problematiku tzv. webcam trollingu, se kterým se často setkávají uživatelé veřejných chatů (Omegle, Chatroulette), ale třeba také uživatelé různých druhů messengerů, které videochat podporují. Princip webcam trollingu je poměrně jednoduchý - pachatel vyzve v online prostředí vyhlédnutou oběť ke komunikaci prostřednictvím webové kamery. Místo skutečného záznamu však oběť vidí předtočenou videosmyčku - muži např. vidí video atraktivní ženy. Oběť, která uvěří, že skutečně komunikuje s osobou, kterou vidí na webkameře, je následně manipulována a sofistikovanými způsoby donucena, aby se před webkamerou obnažila. Vše však pachatel nahrává a citlivý materiál využívá k útoku - vydírání, sexuálnímu nátlaku atd. Oběť, která má strach oznámit situaci policii, pak často platí pachateli za to, že intimní materiály nezveřejní. U dětí pak může dojít např. k vylákání intimních materiálů či přímo k tzv. kybergroomingu.

Diskutující poté samotný webcam trolling v UPointu nasimulovali - prostřednictvím Skypu předvedli, jak snadné je v reálném čase videochat zmanipulovat.

Podle výsledků výzkumu Sexting a rizikové seznamování českých dětí v kyberprostoru (UP, O2 Czech Republic) 22 procent českých dětí potvrdilo, že se před nimi někdo obnažoval na webkameře. Stejně tak téměř 4 procenta dětí potvrdila, že se před webkamerou obnažily. Právě tyto aktivity velmi často vedou k úniku intimních materiálů do prostředí internetu a jejich nekontrolovanému šíření.

Vydírání využívající webové kamery však necílí pouze na děti, terčem se často stávají i dospělí uživatelé internetu - především sociálních sítí. Kpt. Pavel Schweiner, vrchní komisař oddělení kybernetické kriminality olomoucké policie a odborný konzultant a lektor projektu E-Bezpečí, upozorňuje na to, že se terčem vydírání stávají také významní a úspěšní muži. Ti pak raději vyděrači zaplatí nemalý obnos, než aby došlo ke zveřejnění materiálu, který by je mohl velmi poškodit a poznamenat např. jejich kariéru.

Další možností, jak lze webkameru zneužít, představují **různé druhy virových infekcí**, které převezmou kontrolu nad vaší webkamerou a jsou schopny odesílat vaše obrazová data na internet - např. na e-mail pachatele. To je však poměrně technicky obtížné - útočník či případný virus by musel obejít celou řadu technických zabezpečení, od firewallu přes antiviry apod. Není to však nemožné, jak potvrzuje celá řada celebrit, jejichž soukromá fota či krátká videa unikla na internet právě díky virové infekci či přímo hackerskému útoku.

Nejlepším nástrojem, jak se před těmito hrozbami bránit a chránit, je využít kritické myšlení - v žádném případě neplatit vyděrači žádné částky, neposkytovat nikomu (ani svému partnerovi) vlastní intimní materiály, neotvírat neprověřené přílohy emailů či neznámé aplikace pro mobilní doteková zařízení… případně si pořídit třeba krytku na webovou kameru**.**

Redakce E-Bezpečí