E-Bezpečí 2016, 1(2): Page 9-13. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=1173

VELKÉ MNOŽSTVÍ KYBERNETICKÝCH ÚTOKŮ DOKÁŽEME SNADNO ODVRÁTIT – VYUŽÍVAJÍ TOTIŽ LIDSKÝCH CHYB

Kamil KOPECKÝ

V posledních letech se v médiích stále častěji setkáváme s informacemi o internetových hrozbách, kterým jsme neustále vystavováni. Řadu z útoků sami nedokážeme ovlivnit – např. chyby v operačních systémech či počítačových programech nemůžeme bez pomoci specialisty odstranit, musíme si jednoduše počkat na vydání příslušné aktualizace se záplatou. Řadu z internetových hrozeb však dokážeme odvrátit sami – tím, že se jednoduše nenecháme napálit a zachováme se zodpovědně. V následujícím textu si představíme ty nejčastější z nich.

Mezi nejčastější typy online útoků patří **útoky zaměřené na získání citlivých informací uživatelů internetových služeb** (tzv. phishing) – nejčastěji přístupových údajů k účtům elektronického bankovnictví, účtům na sociálních sítích, emailovým účtům apod. Tyto typy útoků probíhají v podstatě každodenně – uživatelé se s nimi setkávají pomocí podvržených bankovních emailů s žádostmi o přihlášení na podvodnou kopii online bankovní služby, podvržené přihlašovací formuláře (např. kopie přihlašovacích obrazovek pro Facebook, Google apod.). Úspěšnost podvodu je přímo úměrná důvěřivosti uživatelů, kteří své osobní údaje internetovým útočníkům poskytnou, aniž by si ověřili autenticitu dané internetové služby.

Dalším klasickým útokem je **infikování počítače počítačovým virem** (tzv. ransomware), který zablokuje přístup k operačnímu systému a žádá po uživateli za odblokování jeho počítače uhrazení

„výkupného“. Výkupné pak musí být uhrazeno prostřednictvím anonymních (či anonymizovaných) platebních služeb. Ransomware se často maskuje jako oficiální zpráva od Policie ČR, která uživateli oznamuje, že porušil zákon (např. stahoval nelegální obsah, sledoval dětskou pornografii apod.), ale že mu trest může být prominut právě uhrazením určitého poplatku (obvykle 2-5000,- Kč). I po uhrazení výpalného však k odblokování počítače obvykle nedojde. Na počátku tohoto útoku je opět lidská chyba – ať již stažení a spuštění infikovaného souboru, absence antivirového programu v operačním systému apod.

Mezi velmi nebezpečné formy internetových útoků, které se v posledních 5 letech v prostředí internetu masově rozšířily, patří **online vydírání uživatelů prostřednictvím intimních materiálů**. O případech online vydírání dětí i dospělých v kyberprostoru informujeme pravidelně prostřednictvím našich internetových stránek a stránek našich partnerů, počet případů v posledních letech vzrůstá (online poradna projektu E-Bezpečí zachytila v průběhu posledních 5 let více než 70 vážných případů vydírání, všechny byly postoupeny k řešení PČR). Vydírání postupuje podle velmi podobných schémat – muž se v prostředí internetu seznámí s „ženou“, naváže s ní intimní kontakt, začne si s ní vyměňovat intimní materiály a po čase přejde i ke komunikaci prostřednictvím webkamery. Postupně jej pak online partnerka přiměje k tomu, aby se před kamerou zcela obnažil. Následně pak virtuální partnerka začne po muži vyžadovat peníze za to, že nezveřejní intimní materiály, které jí muž poskytl. Řada mužů pak částku uhradí, protože nechtějí riskovat, že se jejich záznamy objeví na veřejnosti a poškodí tak jejich pověst. I po úhradě obnosu však v řadě případů vydírání pokračuje dále... Základním problémem tohoto typu útoku je samozřejmě sexting, tedy dobrovolné sdílení intimních materiálů s dalšími uživateli internetu – nejčastěji partnery a partnerkami.

Mezi další formy vydírání, jehož případy jsme zachytili v průběhu června letošního roku, patří **vydírání uživatelů internetových seznamek**. Cílem tohoto útoku jsou zejména zadaní muži, kteří v prostřední online seznamek hledají příležitostný flirt. Celý fenomén jsme popsali na stránkách našeho portálu již dříve, přiblížíme si tedy pouze jeho základní rysy. Uživatel seznamky – muž – se seznámí v online prostředí s ženou, té prozradí řadu

osobních a citlivých údajů o své osobě, mimo jiné i to, že má např. manželku a že hledá flirt či přímo milenku. Následně se stane terčem vydírání – žena mu totiž začne vyhrožovat, že pokud neuhradí konkrétní finanční částku, prozradí jeho manželce, přítelkyni či partnerce informace o tom, že si za ni hledá v prostředí internetu náhradu. Částka, kterou musí muž za udržení tajemství uhradit, se pohybuje v rozsahu od 15000 do 30000 Kč. Pomineme-li etický problém, který je s vyhledáváním potenciálních partnerů a partnerek v prostředí internetových seznamek spojen, důrazně varujeme všechny, kteří v prostředí online seznamovacích portálů hledají své potenciální partnery, aby si uvědomili, jak snadno mohou být citlivé informace, které neznámým osobám sdělujeme, zneužity. A před samotným seznamováním doporučujeme vyjasnit si své aktuální vztahy a předejít tak nepříjemným důsledkům.

Čas od času se v prostředí internetu setkáme také s různými variantami tzv. **scamu** (též scam419, romance scam, nigerijské dopisy apod.). Ačkoli má scam v českém prostředí svůj boom již za sebou, občas narazíme na případ, ve kterém se terčem tohoto podvodu stane např. senior. Podstata scamu je jednoduchá – **pomocí emailu kontaktujeme co nejvíce uživatelů s nabídkou snadného finančního zisku** – fiktivní uživatel nás kontaktuje např. proto, že potřebuje převést ze zahraničí velké množství peněz či zlata, ale nemá dostatek prostředků na uhrazení bankovních poplatků. Proto nabízí za uhrazení těchto poplatků např. procento z celé částky (často milionové sumy), nebo dokonce manželství (uvádí, že je bohatý vdovec, který hledá partnerku, přičemž využívá osamělosti vyhlédnuté oběti apod.). Útočník postupně přiměje oběť, aby mu poskytla finanční prostředky, po jejich uhrazení pak vylákává další a další sumy např. na uhrazení pasu, cla, dopravy, mimořádných výdajů apod. Oběť pak samozřejmě žádné finanční prostředky od pachatele neobdrží.

Za internetovými útoky stojí vždy konkrétní uživatelé (či skupiny uživatelů), kteří využívají jak technických chyb v zabezpečení konkrétních počítačových stanic, tak důvěřivosti jednotlivých uživatelů. Nenechme se zlákat vidinou snadného bohatství či exkluzivní online partnerky, nebuďme přehnaně důvěřiví, snažme se o sobě sdílet co nejméně citlivých informací a veškeré informace si vždy

ověřujme.

Pro E-Bezpečí, Kamil Kopecký