E-Bezpečí 2020, 5(1): Page 73-79. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=1834

VÁCLAV PÍSECKÝ: PODVODNÉ JEDNÁNÍ NAHLÁSÍ POLICII TAK KAŽDÝ DESÁTÝ PODVEDENÝ. LIDÉ SE MNOHDY STYDÍ PŘIZNAT PŘED OSTATNÍMI, JAK NAIVNÍ BYLI NEBO JAK HLOUPĚ SE NECHALI NAPÁLIT.

Kamil KOPECKÝ

Posledních 15 let se zabývá nejzávažnějšími případy spojenými s kybernetickou kriminalitou. Vyšetřuje internetové podvody, ale také mravnostní trestné činy, ke kterým v online prostředí dochází. Dnešní rozhovor jsme vedli s majorem Václavem Píseckým, vedoucím oddělení informační kriminality Služby kriminální policie a vyšetřování Krajského ředitelství hl. m. Prahy.

Jste uznávaným expertem v oblasti internetové kriminality. Co to vlastně kyberkriminalita je a jaké její nejčastější druhy vaše oddělení řeší?

Kyberkriminalita neboli kybernetická kriminalita je souhrnný název pro množinu trestných činů, kdy k spáchání protiprávního jednání byly využity či zneužity prostředky informačních technologií nebo se tyto technologie samy staly cílem útoku. Nejčastěji řešíme kyberkriminalitu z oblasti majetkové (podvody) a mravnostní (problematika zakázané pornografie). Tyto dvě oblasti tvoří cca 80 % veškerého nápadu (výskyt trestných činů za určité období, pozn. red.) na našem oddělení.

Jsou internetové podvody zacíleny pouze na specifickou skupinu obyvatel, nebo se obětí takového jednání může stát kdokoliv?

Obětí internetového podvodu se může stát skoro každý. Je to stejné jako v reálném životě. Největším nebezpečím online podvodů je jejich poměrně veliký dosah. Takový online podvodník poměrně snadno může oslovit stovky nebo tisíce potencionálních obětí. V tomto množství je velká pravděpodobnost, že se nakonec někdo „nachytá“. Navíc takovým bonusem pro online podvodníka je určitě i fakt, že se svými oběťmi nepřichází do fyzického kontaktu.

(Václav Písecký)

O jak vysokou částku mohu přijít, pokud se stanu obětí internetového podvodu?

Přesně o tak velkou, jakou podvodníkovi sami dáte. Lidé se často chovají velmi důvěřivě. Bezmezně věří všemu, co jim kdo předloží.

Nejsou schopni si informace ověřovat, hledat různé informační zdroje a reference. Proto se často stává, že se oběti nachytají i opakovaně. Ne nadarmo se určitým druhům podvodů říká, že je to „daň za lidskou hloupost“.

Kolik lidí každoročně nahlásí, že se stali obětí internetového podvodu?

Celkový počet lidí neznám. Nicméně odhadují, že podvodné jednání nahlásí policii tak každý desátý podvedený. Lidé se mnohdy stydí přiznat před ostatními, jak naivní byli nebo jak hloupě se nechali napálit. Často také mají mylný dojem, že je nějaké nahlášení úplně zbytečné, protože online podvodník nikdy nepůjde vystopovat. Pokud vás ale zajímají čísla, tak přibližně 57 % případů, které Policie ČR řeší v rámci kybernetické kriminality, nese znaky podvodného jednání. Jednoznačně se jedná o největší množinu protiprávního jednání v rámci kyberkriminality.

Velmi často se v rámci kybernetické kriminality hovoří o tzv. phishingu. Co je vlastně je a jak se mu účinně bránit?

Phishing je druhem nebezpečných komunikačních praktik, zaměřených na krádež citlivých osobních údajů - např. PIN kódu a čísel platebních karet, hesla a údaje k bankovnímu účtu a další informace, které by mohly být zneužity. Je to velmi častý způsob, jak se dostat k osobním přístupovým údajům. Nemusí se pokaždé jednat o bankovní systémy, ale například i o přístupové údaje k sociálním sítím, mailovým službám nebo přímo o přístupy do interních firemních systémů. Obrana proti takovému jednání je poměrně jednoduchá – důsledně kontrolovat, kdo se nás na dané údaje ptá, zda stránka, kam tyto údaje zadáváme, není náhodou podvržená. Nesdělovat za žádných okolností naše přístupové údaje komukoliv, kdo by k nim neměl mít nikdy přístup.

Internetová kriminalita se týká také online nakupování. Může si nakupující na internetu nějakým způsobem ověřit, zda je konkrétní e-shop podvodný?

To je velmi těžké otázka. Ale obecně platí pravidlo nakupovat pouze z důvěryhodných zdrojů, využívat uživatelské recenze na daný obchod (i když i tyto často bývají zfalšovány), používat

obchody s jasnou vlastnickou strukturou, kde máte možnost se v případě problému obrátit na konkrétní osoby, ideálně v rámci naší republiky. A především používat „selský rozum“ a nenechat se zlákat nesmyslně nízkou cenou vybraného zboží.

Na internetu jsem objednal zboží ze zahraničí, které mi přišlo poškozené, nebo nepřišlo vůbec. Jak mám postupovat, pokud mě prodávající ignoruje a situaci nechce řešit? Jaká je pravděpodobnost, že své peníze získám zpět?

To bývá často problém. V první řadě je nutné obrátit se na provozovatele obchodu, což může být komplikované i vzhledem k neznalosti místního jazyka. Zahraniční obchody nemají žádnou povinnost s námi komunikovat v naší rodné řeči a angličtina také nemusí být pokaždé z jejich strany akceptována. Spoustu informací ohledně nákupu z ciziny uživatel nalezne na stránkách České obchodní inspekce. Obecně je ale nutné konstatovat, že jakékoli vymáhání náhrad bývá ze zahraničí velmi problematické. Toto by si měl zákazník dobře rozmyslet, než začne nakupovat z neznámých, nejen zahraničních, e-shopů.

Nakupovat tedy u ověřených prodejců. A co dělat, pokud si na e-shopu nebo přes soukromý inzerát koupím zboží, o kterém se později dozvím, že je kradené, bude mi zabaveno? Dostanu v tomto případě své peníze zpět?

Ano, pokud se bude jednat o zboží pocházející z trestné činnosti, je velmi pravděpodobné, že ho policie zajistí po dobu vyšetřování jako důkazní materiál. Náhrada škody může být řešena v rámci trestního řízení, ale častěji bude nutné po skončení trestního řízení zahájit občanskoprávní spor o náhradu škody, což s sebou nese samozřejmě nějaké náklady na soudní poplatky. I když zákazník spor vyhraje a náhrada mu bude určená, není ještě zaručeno, že podvodník tento příkaz dodrží, resp. často se stává, že podvodník peníze již nemá a díky tomu nemá z čeho zaplatit náhradu. Takové případy se pak můžou vléci i několik let. Proto je dobré si podobné nákupy dobře rozmyslet a opět, nenechat se zlákat pouze cenou bez jakýchkoliv záruk.

Dobře. Na internetu se dnes dá koupit téměř cokoli, představme si třeba následující situaci: Koupil jsem přes

internet lístky na koncert. Lupeny mi nepřišly, ukázalo se, že šlo o podvod. Mám kvůli tomu jít na policii, nebo se to kvůli pár stokorunám nevyplatí? Pokud to oznámím, dostanu své peníze zpět?

Určitě má cenu danou věc nahlásit. Je velmi pravděpodobné, že nebudete jediní, komu se podobná věc stala. V konečném součtu se už může jednat o pořádně velkou sumu, kterou přece podvodníkům nenecháme jen tak. Ovšem záruku vrácení peněz vám nikdo nedá. Často se stává, že i když je podvodník vypátrán, peníze již nemá a náhrada škody je problematická a zdlouhavá. Proto opět doporučuji nakupovat i vstupenky na kulturní akce pouze v oficiální distribuci, případně si dobře ověřit jejich platnost.

Na podvodném e-shopu jsem provedl platbu ve virtuální měně (např. Bitcoin). Mám i v tomto případě nárok na náhradu škody?

Samozřejmě, při jakémkoliv protiprávním jednání máte právo na náhradu prokazatelné škody. Nicméně mimo již výše uvedené je zde problém s virtuální měnou. Kryptoměny jako Bitcoin byly navrženy tak, aby nikdo, včetně autorů, jednotlivců, finančních nebo vládních organizací nemohl tyto měny ovlivňovat, zabavovat účty, ovládat či stopovat jejich toky atd. Velmi jednoduše řečeno, Bitcoin je kryptoměna bez jakýchkoliv záruk od státních institucí a sledování pohybu Bitcoinů je víc než problematické, přesněji téměř nemožné. Někomu tyto vlastnosti vyhovují. Jejich největší přednosti ale zároveň mohou být i velkou slabinou. Osobně bych u e-shopů, kde je možnost platby pouze virtuální měnou, raději nic nenakupoval.

(Václav Písecký a Kamil Kopecký upozorňují na riziko internetových predátorů v rámci sexuálně motivované trestné činnosti - foto z doby před nouzovým stavem).

Problém představují také různé druhy podvodných a klamavých reklam. Proč se mi na webových stránkách (např. Seznam.cz, Novinky.cz) objevuje klamavá reklama na podvodné e-shopy? Nestávají se tito provozovatelé kvůli napomáhání spolupachateli?

Bohužel nejsem ten, kdo rozhoduje o umístění reklam na různých webových stránkách, ale mohu pouze odhadovat, že je to z důvodu, že si provozovatel takového podvodného e-shopu na daných stránkách reklamu prostě zaplatil. Toto bývá často krytí podvodných e-shopů. Zaplatí si reklamní prostor na renomovaných a důvěryhodných webových serverech a uživatel pak získá klamný dojem, že když je reklama třeba na Seznamu (internetový portál a vyhledávač, pozn. red.), tak vše musí být v pořádku. Bohužel provozovatelé seriózních internetových služeb často mají prodej reklamního prostoru jako největší zdroj svého příjmu a tento prostor prodají komukoliv, i bez sebemenšího ověření. Často ale prodejci reklamního prostoru nemají možnost poznat, že jde o podvodnou službu.

Na internetu jsem objevil inzerát s nabídkou brigády pro e-shop s elektronikou. Mám založit bankovní účet a budu získávat provize za vyřízené objednávky. Práci jsem přijal a ukázalo se, že šlo o podvodný e-shop. Budu také obviněn?

S největší pravděpodobností ano. A to za legalizaci výnosů z trestné činnosti, případně i za podílnictví. Obecně lze těžko předjímat výsledky vyšetřování a rozhodnutí příslušného soudu. Ale obvinění se téměř jistě nevyhnete. Opět u podobných případů je nutné používat především rozum. Zamyslet se, proč někdo něco takového po mě chce? Proč si toto neobstará sám? Za co přesně je ta odměna? Slangově se pro podobné nastrčené osoby, které mají zakrýt skutečného pachatele, používá výraz „bílý kůň“.

Existují nějaké preventivní programy, které upozorňují na internetové podvody a další projevy kybernetické kriminality?

Doporučuji občas kouknout na stránky České obchodní inspekce, kde je přímo seznam rizikových e-shopů. Mimo to, velmi podrobně se kybernetické kriminalitě, resp. prevenci tohoto jevu, věnuje

projekt E-bezpečí. Samozřejmě i na stránkách Policie ČR najdete spoustu informací a rad, jak se vyhnout případným rizikům v kyberprostoru.

Děkujeme za vaše odpovědi a přejeme klidný zbytek dne.

Kamil Kopecký, Lukáš Kubala
E-Bezpečí