POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra kriminální policie

Podvodné útoky v informačních a komunikačních technologiích

Bakalářská práce

Fraudulent attacks in information and communication technologies.

Bachelor thesis

VEDOUCÍ PRÁCE

plk. v.v. Mgr. Vlastimil Fiedler

AUTOR PRÁCE

Jaroslav ŠÁTEK

PRAHA

2024

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Mladé Boleslavi, dne 22.2.2024

……..

Jaroslav ŠÁTEK

ANOTACE

Bakalářská práce se zabývá podvodnými útoky v informačních a komunikačních technologiích se zaměřením na využití sociálního inženýrství, a to podvodnými investicemi a podvodnými vishingovými útoky označovaných jako „Ruský bankéř“. U uvedených útoků se zabývá legislativou a právní kvalifikací skutků, v dalších částech se práce zabývá neodkladnými a neopakovatelnými úkony pro jejich prvotní prověřování a následné vyšetřování. Uvádí možnosti anonymity telefonních čísel, emailových schránek a IP adres útočníků. V posledních kapitolách se práce zaměřuje především na preventivní opatření, situační prevenci, její současné využití ve společnosti, důležitosti vzdělávání občanů, opatřeními pro policejní orgány v oblasti vzdělávání, ohodnocování a potřebám policistů.

KLÍČOVÁ SLOVA

Sociální inženýrství * podvodné investice * Ruský bankéř * legislativa * anonymita * IP adresa * prevence * vzdělávání *

ANNOTATION

The bachelor thesis deals with fraudulent attacks in information and communication technologies, focusing on the use of social engineering, namely fraudulent investment and fraudulent vishing attacks referred to as "Russian Banker". For these attacks, it deals with the legislation and legal qualification of the acts, while in the following sections the thesis deals with the urgent and non-repeatable actions for their initial screening and subsequent investigation. It presents the possibilities of anonymity of phone numbers, email boxes and IP addresses of the attackers. In the last chapters, the thesis focuses mainly on preventive measures, situational prevention, its current use in society, the importance of educating citizens, measures for police agencies in the field of education, evaluation and the needs of police officers.

KEYWORDS

Social engineering * fraudulent investments * Russian banker * legislation * anonymity * IP address * prevention * education *

Obsah

Úvod

Za téma bakalářské práce byla vybrána problematika internetových podvodů v oblasti elektronické komunikace, a to z několika důvodů. Dnešní populace žije v době 21. století, kterou lze charakterizovat jako dobu exponenciálního růstu elektronické komunikace a rozkvětu internetu prakticky v každém odvětví, tedy i v soukromém sektoru i v domácnostech. Aktuálně dochází k souběžnému žití generace osob důchodového a předdůchodového věku, která z většiny vyrostla ve světe bez internetu, s osobami střední a mladší generace, jež se potkává s internetovým světem takřka od narození. Už z toho lze dovodit, která skupina v největším měřítku vystupuje v pozici útočníků a která v pozici obětí. Ne vždy je cíleno protiprávním jednáním na osoby se sníženým intelektem nebo jakkoliv dočasně či trvale sníženými poznávacími a rozpoznávacími schopnostmi. Zejména u osob první zmiňované skupiny, tedy u osob, jež vyrostly v době jiných společenských poměrů, je využíváno jejich neznalosti a přílišné otevřené důvěřivosti, což bývá alfou a omegou veškerého vznikajícího protiprávního jednání. Dalším důvodem takto zaměřené bakalářské práce je profesní vztah autora přímo k danému tématu, neboť se kybernetické kriminalitě od roku 2017 věnuje jako příslušník bezpečnostního sboru se zařazením na pozici vyšetřovatele u útvaru Policie České republiky, Krajského ředitelství policie Středočeského kraje, Územního odboru Mladá Boleslav, Služby kriminální policie a vyšetřování Mladá Boleslav, Oddělení hospodářské kriminality, se speciálním zaměřením na kybernetickou kriminalitu a taktéž je rozkazem Krajského ředitele policie Středočeského kraje brig. gen. JUDr. Václavem Kučerou, PhD., MBA, členem vyšetřovatelů skupiny vytvořené Krajským ředitelstvím policie Středočeského kraje pro kybernetickou kriminalitu. Fakticky se tak nepřetržitě setkává při každodenní činnosti, jak sofistikovaně a s jakou dynamikou k jednotlivým kybernetickým podvodům dochází. Jelikož ke komunikaci mezi obětí a pachatelem dochází zpravidla dálkově (hlasovým hovorem či elektronickou poštou), lze tyto podvody páchat prakticky z kterékoliv části světa a tato místa libovolně měnit, což i přes nastavenou spolupráci s hraničním přesahem značně komplikuje vlastní vyšetřování. Klíčovou roli hraje i úloha nastupující umělé inteligence (zkráceně AI),

s jejíž pomocí lze dnes za poplatek například anonymně objednat výrobu elektronických osobních dokladů konkrétní osoby po zadání vstupních údajů. Tyto údaje jsou pak některými kryptoměnovými burzami a směnárnami přijímány jako bezvadné validní doklady k registraci kryptoměnových účtů. Díky AI, lze též mimo jiné věrně imitovat hlas konkrétní žijící osoby, čímž vzniká riziko vytvoření dojmu či přesvědčení, že dotyčnou osobu (potencionální oběť) oslovuje jeho rodinný příslušník. Teprve čas ukáže, jaký bude další vývoj u tohoto druhu kriminality, myšleno s využitím AI, a jaké budou na straně zákona vznikat nástroje na její potlačování. Bakalářská práce je zpracována se zřetelem k aktuálnímu období, tj. se zohledněním doposud veřejně deklarovaných zjištěných podvodů a s ohledem na stránkovou omezenost bakalářské práce se zaměřením pouze k vybraným pojmům.

Práce se v teoretické části zaměřuje zejména na ty pojmy, jež budou následně řešeny v její praktické části, jedná se tedy zejména o pojmy spjaté s útoky založenými na principech sociálního inženýrství, možnostech předcházení těmto útokům, IP adresám, komunikační aplikace, aplikace pro vzdálený přístup do zařízení, kryptoměny se zaměřením na kryptoměnu Bitcoin, kryptoměnovou peněženku, kryptoměnové směnárny a peněženky. V další, tj. praktické části práce jsou představovány konkrétní typy podvodných útoků v informačních a komunikačních technologiích, tedy podvodné investice a forma vishingu „Ruský bankéř“ včetně jejich následného prověřování v prvotní fázi, tedy při příjmu oznámení, výslech osoby oznamovatele/oběti a návazné provedení, prvotních neodkladných a neopakovatelných úkonů. Práce řeší především neodkladné a neopakovatelné úkony typu prolomení bankovního tajemství, prolomení údajů o telekomunikačním provozu, zajištění finančních prostředků na bankovních účtech, trasování Bitcoinu a anonymizací telefonního čísla spoofingem a IP adresy. Další částí se autor práce snaží přijít vlastními postřehy, nápady a tipy, jak proti kybernetické kriminalitě bojovat, jak preventivně řešit současný stav. Rovněž se pak zaměřuje na problematiku bezpečnostního sboru a jeho současného stavu v souvislosti s touto problematikou.

Hlavním cílem této bakalářské práce je rešerše informací včetně uvedení osobních zkušeností a postupů autora, seznámení se s podvodnými investicemi

a vishingem „Ruský bankéř“, sběr dat k tématu a jejich popis, následně komparace různých základních atributů útočníka, jakými jsou: webová stránka, doména, email, IP adresa, telefonní číslo, číslo bankovního účtu, kryptopeněženka a další, následně vyhodnocení hodnoty těchto atributů, mimo výše uvedené se práce zabývá též možnostmi aktuálního stavu využití provedené analýzy jednotlivých atributů v prověřování uvedeného útoku, včetně vyhodnocení rizik, negativ a pozitiv. V neposlední řadě pak nastiňuje problémy řešené v souvislosti s kybernetickou kriminalitou v bezpečnostních sborech.

1 Útoky založené převážně na principech sociálního inženýrství

Princip sociálního inženýrství funguje tak, že se pachatel snaží vzbudit důvodné přesvědčení osoby poškozeného o tom, že mu může plně důvěřovat. Pachatel dále s poškozeným pomocí různých emocionálních nátlaků, psychologicky manipuluje, aby docílil svého záměru. Tím je nejčastěji získání finančních prostředků, údajů k zabezpečeným účtům oběti, přístupové údaje k jeho bankovnictví, do sociálních sítí, emailu apod. Jedná se též o získání osobních údajů oběti, kopie jejích dokladů, případně identity jako takové, kdy se následně pachatel vydává za poškozenou osobu, aby mohl páchat další trestnou činnost (např. legalizace výnosů z trestné činnosti).[1]

Ve světě je znám pojem sociální inženýrství, a to pod názvem social engineering, human hacking. Pro účely této práce je důležitý přímo pojem útok pomocí sociálního inženýrství. Sociální inženýrství je ve světe a v České republice vedeno jako jedna z největších bezpečnostních hrozeb, a to jak pro jednotlivce, tak pro systém jako takový, kterým společnosti čelí. Jedná se o velmi efektivní jednání, které využívá přesvědčivé a lživé útoky.

Nedávná zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022, aktuální a poslední vydaná dne 19.7.2023, Národním úřadem pro kybernetickou a informační bezpečnost mimo jiné uvádí: „*Během roku 2022 došlo k mírnému snížení kybernetických incidentů evidovaných NÚKIB ze 157 na 146, nicméně Policie České republiky zaznamenala téměř dvojnásobný nárůst kyberkriminálních aktivit. Největší hrozbu pro kybernetickou bezpečnost České republiky pak i nadále představují aktivity státem sponzorovaných kybernetických aktérů a činnost kyberkriminálních uskupení.*“[2]

---

[1] DONÁT, Josef, TOMÍŠEK Jan, PRÁVO V SÍTI, průvodce právem na internetu, Praha: C. H. Beck, 2016, ISBN 978-80-7400-610-4, str. 260. [citováno 2024-02-09].

[2] KINTR, Lukáš. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022*. Online. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Dostupné z: https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/, str. 1, [citováno 2024-02-09].

Z aktuálnější zprávy vydané Policií České republiky dne 12.1.2024 cituji:

„Kriminalita páchaná v kyberprostoru v roce 2023 stále tvoří 10,8 % celkové registrované kriminality. Dle statistických dat je tento trend setrvale stoupající (meziročně +0,6 %, +1 038 skutků), přesto však oproti předchozím rokům jde o vzestup podstatně nižší. Objasněnost v této oblasti kriminality poklesla meziročně o 1,3 %. Opakovaně jsme zaznamenali pokles případů tzv. hackingu (- 939, -33 %). Lze předpokládat, že skutky spáchané v dané oblasti jsou i tzv. souběhové s majetkovou trestnou činností.

V oblasti podvodů páchaných v online prostředí se stále setkáváme s provázanou sériovou trestnou činností. Typický je nábor legalizátorů výnosů z trestné činnosti na sociálních sítích a dalších online platformách. Phishing probíhá skrze emailovou komunikaci, sociální sítě a placenou inzerci na webových stránkách. Speciální variantou je phishing v podobě podvodných telefonátů a SMS zpráv. V podvodných telefonátech významně převažuje legenda falešného bankéře ve spojení s legendou napadeného bankovnictví. V těchto případech je často využíván vzdálený přístup k zařízení oběti a následný vklad peněz oběti do vkladomatů na virtuální měny. Přetrvává rozesílání podvodných SMS zpráv, které předstírají, že jsou zasílány institucemi nebo přepravními společnostmi. Cílem je vylákat přístupové údaje do internetového bankovnictví oběti a neoprávněně odčerpat její finanční prostředky. V současnosti zaznamenáváme nárůst případů s velmi nebezpečným modem operandi, a to kombinací podvodné SMS zprávy a podvodného telefonátu.“[3]

Pachatel může sledovat digitální stopu svých obětí, což je sada informací, kterou zanechá uživatel internetu v internetové síti i lokálních IT a elektronických zařízeních.[4] Tím může pachatel vědět o potencionální oběti více informací, které může zneužít právě k navození důvěry, útok je pak cílenější a daleko nebezpečnější, než když informace z digitální stopy nemá, protože je musí pak během

---

[3] VINČÁLEK, Jakub a MORAVČÍK. Ondřej. *Policie České republiky: Vývoj registrované kriminality. v roce 2023.* Online. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2023.aspx [citováno 2024-02-09].

[4] Digitální stopa. *IT Slovník*. Online. Dostupné z: https://it-slovnik.cz/pojem/digitalni-stopa. [citováno 2024-02-09].

komunikace s obětí během hovoru postupně získávat. Pachatelé činí soustavné jednání nebo dokonce celé nábory potencionálních obětí, a to buď přímo cílené na určitou osobu (příklad RomanceScam[5]) nebo skupinu lidí (příklad podvodné investice, podvodné mobilní platby).[6]

Vektorem útoku, myšleno jako způsobem útoku, je v zásadě způsob, jakým dochází ke zneužití zranitelnosti a kompromitaci cílové osoby. Může se jednat o spam, tj. náhodně cílenou nevyžádanou zprávu a komunikaci. Odesílatel takové komunikace a zprávy se často jeví jako uznávaná osobnost, např. veřejně známá osobnost jako prezident, premiér, lékař, sportovec, nebo solventní a úspěšná společností, např. banka, státní orgán, Agrofert, ČEZ, tedy z pohledu adresáta se jedná o uznávané autority. Nejčastější typy útoků jsou v současné době páchány přes reklamu na sociálních sítích, či internetových stránkách (například Facebook, YouTube), což můžeme zařadit do takzvaných phishingových kampaní, pod něž lze podřadit taktéž specifické podsekce jako klasický phishing, vishing, smishing a podobně.[7]

Útoky sociálního inženýrství velmi dobře fungují, jelikož využívají, jak je výše uvedeno, lidské zranitelnosti, zejména strachu a časového nátlaku, jelikož lidé jednají pod vlivem strachu a časové tísně jinak, než by reagovali normálně, tedy naprosto neadekvátně. Můžeme se setkat i s paradoxy typu, čím více peněz na účtu oběť má, tím je daleko vyšší pravděpodobnost, že o tyto peníze přijde. Působení a vliv strachu má totiž na oběť silnější působnost. Jiná je situace, kdy pachatel v oběti vyvolává pocit vzájemnosti, reciprocity, kdy oběť má tendenci oplácet laskavost a pachatel toho využije (např. falešné finanční sbírky, pomoc v tísni kamarádům, příbuzným).

---

[5] Romance Scam. Policie České republiky. Online. Dostupné z: https://www.policie.cz/soubor/romance-scams.aspx. [citováno 2024-02-09].

[6] KOLOUCH, Jan. *CyberCrime*. Online. Praha: CZ.NIC, 2016.ISBN 978-80-88168-18-8. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf str. 186-188. [citováno 2024-02-09].

[7] KINTR, Lukáš. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022*. Online. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Dostupné z: https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/, str. 18. [citováno 2024-02-09].

Oběť často jedná až do konce jednání, které pachateli slíbí, protože cítí závazek a pachatel cílí na pocit důslednosti, dodržení slova oběti, proto je pravděpodobnější, že oběť dohodu s pachatelem splní a celý proces útoku takto pachatel dokončí. Pachatelé spoléhají na sociální tlak vytvořený na své oběti, což se dále projevuje například i tak, že oběť čte komentáře a recenze (fiktivní a smyšlené, vytvořené samozřejmě pachatelem) pod určitými nabídkami, inzercí, reklamními upoutávkami, a získá potřebu, dělat to, co dělají ostatní lidé či jeho známí, a získat tak proklamovaný profit. Jedná se o prostý fakt, že lidé jsou ve své podstatě chamtiví, chtějí se mít lépe, v touze po rychlém zisku s vynaložením minimálního úsilí, jednají zaslepeně a bezmezně důvěřují svému momentálnímu úsudku, ačkoliv ten je již ovlivněn pachatelem skrytým za lákavou reklamou či nabídkou. Paradoxně, což dokládá i praxe, svému (pachatelem ovlivněnému) úsudku věří často i vzdělaní lidé, jelikož oni jsou přece „ti chytřejší". Na vnímání obětí má vliv mimo jiné i zdánlivá nedostupnost služby či zboží, exkluzivita či časová omezenost nabídky, což se projevuje tak, že v nabídkách pachatelů se objevují výrazy jako „poslední možnost", „pouze pro posledních pár lidí", „poslední šance" a podobně.[8]

[8] DONÁT, Josef, TOMÍŠEK Jan, *PRÁVO V SÍTI, průvodce právem na internetu*, Praha: C. H. Beck, 2016, ISBN 978-80-7400-610-4, str. 261. [citováno 2024-02-09].

2 Pojmy a nástroje důležité pro útoky založené na principech sociálního inženýrství

K problematice útoků založených na principech sociálního inženýrství se pojí mnoho programů, pojmů a nástrojů, mnoho z nich je veřejně známých a dostupných, ale několik z nich je si třeba představit, neboť se jedná o jisté základní kameny pojmosloví a jejich vymezení je vhodné pro celkovou koncepci této práce. Vzhledem k jejich množství, bylo vybráno jen několik těchto pojmů, a to těch, jež se používají nejčastěji. Právě tyto pojmy se v útocích s využitím sociálního inženýrství i ve všech podvodných útocích v informačních a komunikačních technologiích opakují a jsou nejčastěji zastoupené.

2.1 IP adresa

Jedná se o jeden z nejdůležitějších atributů, kterým se v internetovém prostředí identifikuje zařízení přihlašující se do sítě internet. IP je zkratka pro Internet Protokol (nejzákladnější síťový protokol, který zabezpečuje doručování dat v síti). IP adresu lze chápat jako unikátní číselný kód, který umožňuje jednoznačně určit zařízení, které přes internet komunikuje. IP adresa slouží ke komunikaci a lokalizaci zařízení v síti (lze ji považovat za podobný údaj jako je adresa uvedená na poštovní obálce). Můžeme je rozlišovat dle anonymizace a jiných atributů.

2.2 Komunikační aplikace

Komunikačními aplikacemi rozumíme aplikace typu Facebook messenger[9], WhatsApp[10], Telegram[11], Viber[12] a jim podobné aplikace, které jsou volně dostupné pro

---

[9] Facebook Messenger. META. *Facebook.com.* Online. Dostupné z: https://www.messenger.com/features?locale=cs_CZ. [citováno 2024-02-09].

[10] WhatsApp, WHATSAPP IRELAND LIMITED. *Whatsapp.com*. Online. Dostupné z: https://www.whatsapp.com/?lang=cs_CZ. [citováno 2024-02-09].

[11] Telegram. *Telegram.org.* Online. Dostupné z: https://telegram.org/. [citováno 2024-02-09]

[12] Viber. VIBER MEDIA. *Viber.* Online. Dostupné také z: https://www.viber.com/en/. [citováno 2024-02-09].

širokou veřejnost, mají různé úrovně zabezpečení a možnosti využití, kdy v určitých zemích se používají v různé míře, například aplikace Telegram je využívána zejména ve východní Evropě pro její oblíbenost mezi tamější populací, zatímco trend v České republice stále zůstává a převládá v aplikacích Facebook messenger, Instagram, Whatsapp. K užívání těchto aplikací je třeba pouze přítomnost uvedené aplikace v zařízení a internetové připojení.

2.3 Aplikace pro vzdálený přístup do zařízení

Aplikacemi pro vzdálený přístup do zařízení rozumíme především programy AnyDesk[13], TeamViewer[14], SupRemo[15], které jsou veřejně dostupné na internetu. Uvedené programy stačí do zařízení stáhnout, a to i do mobilního telefonu, tedy nejen do stolního počítače, či notebooku. Po přihlášení do uvedených aplikací se uživateli (potenciální oběti) zobrazí identifikační číslo – pokud toto číslo sdělí druhému uživateli, který má aplikaci také staženou a otevřenou, připojí se tento druhý uživatel vzdáleně svým zařízením do zařízení uživatele prvního. Tímto způsobem následně vidí druhý uživatel na svém zařízení monitor zařízení prvního uživatele a může jej plně, či omezeně ovládat. Míra ovládání záleží na nastavení aplikace, přičemž uživatel dávající přístup může převzít nad svým zařízením kontrolu zpět. K užívání těchto aplikací je třeba pouze přítomnost uvedené aplikace v zařízení a internetové připojení.

2.4 Kryptoměna

Kryptoměna je forma digitální, virtuální měny, která využívá kryptografii pro zabezpečení transakcí, regulaci vytváření nových jednotek a ověřování

---

[13] AnyDesk. ANYDESK. *Anydesk.com.* Online. Dostupné z: https://anydesk.com/en. [citováno 2024-02-09].
[14] TeamViewer.TEAMVIEWER. *TeamViewer* . Online. Dostupné také z: https://www.teamviewer.com/cs/. [citováno 2024-02-09].
[15] SupRemo. NANOSYSTEMS. *SupRemo.* Online. Dostupné také z: https://www.supremocontrol.com/. [citováno 2024-02-09].

převodu aktiv. Na rozdíl od tradičních měn není kryptoměna fyzickým objektem a neexistuje v tradiční podobě bankovek a mincí. Místo toho jsou všechny informace o vlastnictví a transakcích uloženy v digitální podobě na blockchainu, který je decentralizovaný a transparentní systém. Bitcoin byl první kryptoměnou, která byla představena v roce 2009. Od té doby vzniklo mnoho dalších kryptoměn, včetně Ethereum, Ripple, Litecoin a dalších. Kryptoměny se staly předmětem široké diskuse kvůli svému potenciálu změnit způsob, jakým probíhají finanční transakce, a také kvůli otázkám týkajícím se regulace, bezpečnosti a stability.

2.5 Bitcoin

Pro účely znázornění problematiky virtuálních měn používaných při páchání podvodných útoků v informačních a komunikačních technologiích se práce zaměří na kryptoměnu Bitcoin, jelikož se jedná o nejstarší a nejznámější kryptoměnu svého druhu s fundamentální hodnotou a jelikož na významu podvodů co do druhu tyto probíhají s ostatními kryptoměnami v jádru totožným způsobem. Mění se tedy zpravidla jen název kryptoměny a přirozeně její jednotka. Bitcoin byl tedy zaveden v roce 2009, uživatelem/skupinou pod pseudonymem Satoshi Nakamoto[16]. Poprvé byl popsán v roce 2008. Bitcoin byl navržen jako decentralizovaný systém elektronických plateb, který umožňuje přímé převody mezi dvěma stranami bez potřeby prostředníka, jako jsou banky nebo platební brány. Bitcoin se stal subjektem intenzivního zájmu kvůli svému potenciálu stát se platebním prostředkem nezávislým na stávajícím finančním systému, ale také kvůli obavám týkajících se bezpečnosti, regulace a otázek ohledně energetické náročnosti těžby. Mnoho dalších kryptoměn se od té doby objevilo a každá z nich má své vlastní jedinečné vlastnosti a účely.[17]

---

[16] STROUKAL, Dominik a SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. *Třetí rozšířené vydání*. *Finance pro každého*. Praha: Grada Publishing, 2021. ISBN 978-80-271-1043-8. str. 28-29. [citováno 2024-02-09].

[17] Bitcoin. BITCOIN. *Bitcoin.* Online. Dostupné také z: https://bitcoin.org/en/. [citováno 2024-02-09].

2.6 Kryptoměnová peněženka

Kryptoměnová peněženka (nebo také kryptopeněženka) je digitální nástroj, na který je možné ukládat kryptoměny, dále je také možné z jedné na druhou kryptopeněženku zasílat kryptoměny. Je možné si je představit jako digitální verzi fyzické peněženky, kde uživatelé uchovávají své peníze. V případě kryptopeněženky jsou to právě kryptoměny. Kryptopeněženky mohou být ve formě hardwarových zařízení (fyzické peněženky), softwarových aplikací (desktopové, mobilní aplikace nebo online peněženky), nebo dokonce papírových dokladů s natištěnými klíči.[18]

2.7 Kryptoměnové směnárny

Kryptoměnová směnárna (také nazývaná kryptoměnová burza, kryptoburza nebo kryptoobchod) je platforma ve virtuálním prostředí, přes kterou mohou uživatelé obchodovat právě s uvedenými kryptoměnami. Jedná se o směnárny, ke kterým si uživatel připojí svou vlastní kryptopeněženku nebo mu jí směnárna sama vytvoří, a následně v rozhraní webových stránek může uživatel v reálném čase za určitý transakční poplatek dále s kryptoměnami nakládat, prodávat je, nakupovat, směňovat mezi sebou za ekvivalent tržní hodnoty kryptoměny, kterou nabízí a kterou poptává. Kryptoměnové směnárny nedílnou součástí kryptoměn, kdy se jedná o nejsnadnější možnost k získání kryptoměny. Příkladem některých

---

[18] STROUKAL, Dominik a SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. Třetí rozšířené vydání. Finance pro každého*. Praha: Grada Publishing, 2021. ISBN 978-80-271-1043-8. str. 76-99. [citováno 2024-02-09].

známých kryptoburz jsou Binance[19], Coinbase[20], Kraken[21], Bitstamp[22] a mnoho dalších. Každá kryptoburza má různý stupeň kvality, rychlosti, poplatků a zabezpečení, proto je velmi důležité, kterou si uživatel vybere a pro policejní orgán, kde uvedená kryptoburza sídlí a zda spolupracuje s orgány činnými v trestním řízení.

---

[19] Binance. BINANCE. *Binance*. Online. Dostupné také z: https://www.binance.com/cs. [citováno 2024-02-09].
[20] Coinbase. COINBASE. *Coinbase*. Online. Dostupné také z: https://www.coinbase.com/. [citováno 2024-02-09].
[21] Kraken. PAYWARD, INC. *Kraken.* Online. Dostupné také z: https://www.kraken.com/. [citováno 2024-02-09].
[22] Bitstamp. BITSTAMP USA, INC. *Bitstamp*. Online. Dostupné také z: https://www.bitstamp.net/. [citováno 2024-02-09].

3 Podvodné investice

Podvodných útoků v informačních a komunikačních technologiích je nepřeberné množství, můžeme zmínit třeba, phishing, smishing, spear phishing, vishing, CEO a BEC útoky, podvodné mobilní platby, RomanceScam/Scam 419, reverzní inzertní podvody, a právě podvodné investice, kterým se bude práce věnovat v dalších částech. Z autorových zkušeností vyplývá, že podvodné investice[23] jsou specifickým druhem útoku, který cílí na finanční prostředky zejména fyzických osob, jež vyhledává i za využití sociálního inženýrství v internetovém prostředí. Principem je vylákání finančních prostředků pod záminkou nejrůznějších vysoce výnosných investic, zejména se jedná o podvodné investice do akcií známých firem (Agrofert, ČEZ, Apple, Tesla a podobně), dále pak do různých komodit (virtuální měny, především Bitcoin, Ethereum), jaderná energie, ropa, robotizace, burzy komodit jako jsou obilí, dřevo a podobně. Jedná se o cílenou reklamu v internetovém prostředí zejména na sociálních sítích, kde se pachatelé zaštiťují známými osobnostmi (bez jejich vědomí) s přirozenou autoritou, dobrou pověstí či obecnou popularitou (například bývalý premiér a současný politik Andrej Babiš, miliardář Elon Musk, Bill Gates a podobně). Potencionální oběť tedy zareaguje na uvedenou reklamu, která využívá veškerých principů sociálního inženýrství, viz výše, a která oběť přesměruje mimo sociální síť na webové stránky útočníka (např. 3g-in.cc, Elleon-capital.com, guardianinvest.co, bbprofit.co, skills-profit.com, globalnews trade, Foxgloballtd.com, trade-union, Atlantik-star.com, capital-star,i-deal-group, moonstrade a podobně).

Webové stránky se jeví velmi důvěryhodně a propracovaně, nesčetněkrát se na nich nachází i falešné recenze spokojených investorů, na stránkách je možné se zaregistrovat vyplněním několika údajů jako je jméno, příjmení, ale především emailu a telefonního čísla. Po zadání údajů se za nějaký čas (může to trvat minuty, hodiny nebo také třeba dny) oběti ozve investiční poradce, který se představí jménem společnosti a dost často i svým falešným jménem, následně

---

[23] BURÝŠEK, Jiří. YOUTUBE – KANÁL JIRKA VYSVĚTLUJE VĚCI. *Poslal jsem podvodníkovi 300 000 Kč*. Online. Dostupné také z: https://www.youtube.com/watch?v=bre2eJsAdhM. [citováno 2024-02-09].

začne s poškozeným komunikovat ohledně toho, do čeho je možné se společností investovat a jaké jsou možnosti zhodnocení peněz. V blízké době od započetí hovoru poradce kontaktuje oběť také prostřednictvím komunikačních aplikací, kde oběti může zasílat přímé odkazy, falešné písemnosti a dále s ní komunikovat. Při komunikaci s obětí se údajný poradce velmi často snaží vylákat z oběti informace o jejím rodinném stavu, finančních možnostech, majetku, bankovních účtech a podobně. Pokud pak oběť k fiktivnímu investování přesvědčí, zpočátku po ní požaduje jen malé částky v řádech několika tisíců korun. Po prvotním vkladu, který poškozený učiní buď na bankovní účet v České republice, či na bankovní účet v zahraničí, nebo přímo přes různé transakční aplikace na kryptopeněženky, ovládané právě údajným finančním poradcem (viz výše bod. 2.4 - 2.7) nebo dalším členem jeho skupiny, je ve většině případů oběti doručeno důvěryhodně vyhlížející potvrzení o přijetí platby. Jedná se o falsum, které však v oběti ještě více podpoří důvěru v pachatele a zároveň ji zbavuje podezření, že by se mohlo jednat o podvodné jednání. Následuje odeslání internetového odkazu oběti, poté, co na odkaz oběť klikne, je přesměrována právě na předmětné webové stránky, oběť je dále vyzvána k zaslání svých přístupových údajů, čímž se na webových stránkách přihlásí do rozhraní, kde jsou oběti ručně zapsány finanční prostředky. Oběť v tuto chvíli vidí, jak jím zaslané finanční prostředky na webových stránkách vydělávají a získávají na hodnotě na různých grafech, diagramech. Po „utopení“ prvních investovaných finančních prostředků poradce za několik dní opět kontaktuje oběť (většinou telefonicky) a přesvědčuje ji k dalším investicím, požaduje již vyšší finanční částky. Zde je zajímavé, že pachatelé se zaměřují na princip „utopených peněz“ - poškozený již nějaké peníze investoval, vidí, jak mu vydělávají a že je to velmi výhodné. Oběť, která zpočátku hodlala investovat jen malé množství svých finančních prostředků, se tedy následně nechá zlákat na další investice, a to v podstatně vyšší částce (částkách). V případě, že oběť neovládá a nerozumí IT prostředí, či se neorientuje v některém z kroků při zasílání finančních prostředků, registrace na webových stránkách, nebo na bankovních platformách, přes něž chce poradce finanční prostředky zasílat, je jí ze strany údajného investičního poradce nabídnuta podpora a pomoc za využití aplikace pro vzdálený přístup do zařízení. Oběti je zaslán přes komunikační aplikaci oběti odkaz na stažení aplikace

pro vzdálený přístup do zařízení, současně je během hovoru vyzvána, aby poradci sdělila kód na tuto aplikaci. Po jeho sdělení převezme údajný poradce kontrolu nad zařízením oběti. Zde pak jedná za oběť a vše explicitně vysvětluje. Je-li oběť ochotná investovat vyšší finanční částky, poradce jí velmi ochotně radí nebo dále i pomáhá finanční prostředky zasílat. Oběť se sama přihlásí do svého bankovního účtu a následně vše vykonává pod dohledem a s pomocí poradce. Nezřídka nastanou i situace, kdy poradce přiměje oběť, aby na investování finančních prostředků vzala půjčku, i s vyřízením půjčky jí taktéž výše popsaným způsobem údajný poradce pomůže. Oběť tedy dále postupně investuje své finanční prostředky až do bodu, kdy jí tyto buď dojdou, tedy žádné další už investovat nemůže, anebo do bodu, kdy by oběť chtěla zhodnocené finanční prostředky vybrat ze svých bankovních účtů. V tu chvíli poradce oběť rafinovaně přemlouvá, aby investovala dál, nebo zisk nebude tak vysoký, případně oběti sdělí, že pro výběr zhodnocených finančních prostředků je třeba zaplatit daň. Ve většině případů již oběť žádné finanční prostředky nemá, proto se jí poradce opět snaží přesvědčit do uzavření půjčky, úvěru, popř. zastavení nemovitosti, prodeji jiného majetku apod., pod legendou, že po zaplacení daně se zhodnocené finanční prostředky uvolní a zašlou oběti na účet. V této chvíli ve většině případu oběť procitne a dojde jí, že o veškeré investované finanční prostředky přišla a vše oznámí svému okolí, nebo přímo Policii České republiky. Uvedený podvod s investicemi je jeden z nejrozšířenějších po celé České republice i v zahraničí, kdy autor práce zpracovával větší množství těchto podvodů, neboť metodicky vedl kolegy z obvodních oddělení na územním odboru Mladá Boleslav. [24] [25] [26]

---

[24] BLAHNÍKOVÁ, Irena. VLTAVA LABE MEDIA. *Boleslavský deník*. Online. Dostupné také z: https://boleslavsky.denik.cz/zlociny-a-soudy/boleslavsko-podvod-kdyptomena-investice-policie-cr-20062023.html. [citováno 2024-02-09].

[25] BLAHNÍKOVÁ, Irena. VLTAVA LABE MEDIA. *Boleslavský deník*. Online. Dostupné také z: https://boleslavsky.denik.cz/zlociny-a-soudy/mlada-boleslav-policie-cr-podvodnici-prehled-pripady-rok-2023-05012024.html?cast=3 (a části 4–5). [citováno 2024-02-09].

[26] CHAROUSKOVÁ, Šárka. STATUTÁRNÍ MĚSTO MLADÁ BOLESLAV. *Mb-net*. Online. Dostupné také z: https://mb-net.cz/internetovi-podvodnici-pripravili-muze-z-boleslavi-o-pul-milionu-korun/d-78260/p1=63082. [citováno 2024-02-09].

4 Podvodný útok „Ruský bankéř“ – Vishing

Z autorových zkušenost je dalším velmi rozšířeným podvodným útokem v informačních a komunikačních technologiích takzvaný „Ruský bankéř“, uvedený skutek se takto v policejních kruzích, i mimo ně, označuje především proto, že zpočátku se útočníci velmi dobře identifikovali ruským či jinak „východním“ přízvukem, nebo se zaměřovali na občany států východní Evropy, zemí bývalého Sovětského svazu. Následně bylo zjištěno, že útočníci se nacházeli na území Ukrajiny, kde byli taktéž za mezinárodní spolupráce vypátráni a vydáni do České republiky.[27]

Ve věci se jedná o soustavné a koordinované jednání útočníků, kteří jsou výborně organizováni. Útočníci získají důležité informace o obětech, a to zejména jejich telefonní čísla v internetovém prostředí, buď po úniku dat z bankovních či jiných společností (hackingu). Jako příklad můžeme uvést:

„2013: Korporátní databázi softwarové firmy Adobe Systems se podařilo napadnout a získat přihlašovací údaje k účtům. Únik dat se dotkl celkem 38 000 000 aktivních uživatelů.

2014: Hackeři podnikli cílený útok na uživatelská jména, hesla a bezpečnostní otázky slavných lidí a následně zveřejnili téměř 200 soukromých fotografií celebrit-

2014: Aukční server eBay oznámil únik 145 000 000 záznamů o uživatelích. Hackeři se nejprve nabourali jen do několika zaměstnaneckých účtů, přes ně pak pronikli do korporátní sítě.

2015: Britský poskytovatel telefonních služeb čelil útoku skupiny pouze patnáctiletých hackerů, které se ovšem podařilo ukrást informace o zhruba 4 000 000 zákazníků.

---

[27] HRABĚ, Jan. INCORP A. S. *Ukrajina předala české policii pětici osob, má jít o podvodníky.* Online. Dostupné také z: https://eurozpravy.cz/domaci/ukrajina-predala-ceske-policii-petici-osob-ma-jit-o-podvodniky.e3vk52tb. [citováno 2024-02-09].

2016: Skupině hacktivistů se podařilo vizuálně změnit internetové stránky filipínské volební komise. Jiná skupina pak nahrála celou databázi webu na Facebook"[28]

Dále také třeba úniky dat klientů ze samotných bank, což je velmi vážné jednání a velmi významné bezpečnostní pochybení bank.[29]

Vishingový útok, což je zkratka pro „Voice Phishing", je cílený útok sloužící k získání citlivých informací od oběti, například jména, příjmení, rodného čísla, adresy bydliště, čísla bankovního účtu, čísla platební karty, přihlašovacích údajů do bankovnictví a podobně. Útočníci vystupují pod jinou identitou. Cílem útočníků je tedy vylákat citlivé údaje oběti, vylákat z ní smyšlené pohledávky a poplatky, přimět oběť k provedení transakce či jiné činnosti k převodu finančních prostředků, přimět ji ke stažení aplikací pro vzdálené ovládání zařízení a následně umožnění vzdáleného přístupu do zařízení oběti, nalákat na nevýhodný či podvodný marketing.

Útoky vishingu můžeme rozdělit na cílený útok a na plošný útok. Cílený útok znamená, že pachatel již zná informace o své oběti, proto je tento útok nebezpečnější, můžeme jej označit jako Spear vishing. Zatímco plošný útok je takový, kdy pachatel volává na náhodně vybraná telefonní čísla nebo využívá umělou inteligenci „robota – BOTa" který předá přes hovor předem namluvenou informaci, oběť pak sama reaguje zavoláním na určité telefonní číslo, kde je následně spojena s útočníkem nebo reaguje přímo podle instrukcí BOTa.

Útočník „Ruský bankéř" využívá zjištěných osobních dat o klientech bank, zejména za využití telefonního čísla a jména budoucí oběti, které zjistí buď výše uvedeným jednáním anebo jinými veřejně dostupnými sdělovacími prostředky, prostřednictvím internetu a podobně. Kombinuje prvky cíleného i plošného útoku, ale následně přechází do reálného jednání útočníka (ne BOTa) Taktéž využívá veřejně známá jména zaměstnanců bank, a to i České národní banky. Následně

---

[28] MBANK S.A. *Krádeže osobních údajů*. Online. Dostupné také z: https://www.mbank.cz/blog/post,735,kradeze-osobnich-udaju.html. [citováno 2024-02-09].

[29] KŘÍŽEK, Martin. IROZHLAS. *Únik dat klientů Komerční banky je opravdu vážné pochybení, říká právník z Iuridicum Remedium*. Online.Dostupné také z: https://www.irozhlas.cz/zpravy-domov/unik-dat-klientu-komercni-banky-je-opravdu-vazne-pochybeni-rika-pravnik-z-iuridicum-remedium_201307231846_vkourimsky. [citováno 2024-02-09].

kontaktuje telefonicky oběť, kdy se představí jako člen bezpečnostního oddělení České národní banky, zeptá se oběti na to, zda je u určité banky. Oběť sdělí, že ne, že má účet i jiné banky, na to útočník reaguje sdělením, že tímto se právě odhalilo, podvodné jednání a že se bude snažit oběti ochránit finanční prostředky na jejích účtech. Protože již zná banku oběti (ta mu jí sama sdělila), přepojí (přesměruje hovor) oběť na dalšího útočníka, který se již představuje jako bezpečnostní technik banky oběti, dále pak komunikuje s obětí prostřednictvím telefonního hovoru a případným využitím komunikačních aplikací, kdy přesvědčí oběť, že si na jejím bankovním účtu chtěl neznámý pachatel vzít půjčku nebo že banka eviduje podezřelé platby do zahraničí a vyhodnotila žádost nebo platby jako rizikové, proto oběti volají, aby společně „zachránili" finanční prostředky na účtech oběti. Pokud je oběť dále nedůvěřivá, tak jí sdělí, že jí zavolá policejní komisař, který jí zavolá z telefonního čísla jevícího se jako telefonní číslo Policie České republiky, představí se jako policista vyšetřovatel a sdělí dále oběti, aby o celé věci s nikým jiným nehovořila, že se jedná o policejní vyšetřování spojené s ochranou osobních údajů. Oběť má důvěřovat jen bezpečnostnímu technikovi banky a taktéž uvedenému vyšetřovateli, Bezpečnostní technik následně přesvědčuje oběť, aby vybrala všechny finanční prostředky ze svých účtů, kdy jí poradí nebo pomůže prostřednictvím aplikací pro vzdálený přístup do zařízení zvednout limity pro výběr finančních prostředků. Případně nutí oběť finanční prostředky přeposlat na „bezpečný" účet banky, který ale samozřejmě plně ovládá útočník. Během celého jednání využívá metod sociálního inženýrství, kdy oběť přesvědčuje i o tom, že pachatel může být rovněž mezi pracovníky banky. Tohoto sdělení následně využívá k tomu, aby oběť vybrala finanční prostředky ze své banky. Při výběru větších finančních obnosů útočník oběti poradí, aby výběr odůvodnil např. koupí vozidla nebo jinou legendou. Zde se setkáváme s nejslabším článkem v provedení útoku, jelikož mnoho poškozených se právě v tomto bodě obrací na skutečného bankéře v bance, který mu sdělí, aby celou věc neprodleně oznámil na Policii České republiky. Pokud však oběť přesto finanční prostředky vybere a má je u sebe v hotovosti, snaží se ji útočník dále přesvědčit, aby si sjednala v bance co největší možnou před schválenou půjčku, což odůvodňuje „bonitou nebo bonifikací" pro další zajišťování a záchranu finančních prostředků. I zde shledáváme další slabou

část v jednání útočníka – mnoho obětí si uvědomí, že půjčku si brát nehodlají, obrátí se opět na skutečného bankéře, rodinu nebo Policii České republiky. Pokud útočník přes všechny výše uvedené alternativy přece jen oběť přesvědčí k uzavření půjčky či k výběru vysoké částky finančních prostředků z jejího účtu, je velmi pravděpodobné, že mu celý útok vyjde. Sdělí oběti, aby dojela k nejbližšímu bitcoinmatu, což je fyzický bankomat na nákup a prodej kryptoměny. Prostřednictvím internetu útočník vytvoří kryptopeněženku a její QR kód zašle komunikační aplikací oběti. Ta mu pak na jeho výzvu u bitcoinmatu QR kód naskenuje, do bankomatu vloží své finanční prostředky a tím je nenávratně zašle na krypotopeněženku útočníka. Pokud útočník k sjednání úvěru nepřesvědčil oběť již před tímto jednáním, snaží se ji přesvědčit právě po zaslání těchto finančních prostředků, nejčastěji pod legendou zaplacení poplatků a daní z platby, nebo požaduje po oběti zaslání ještě vyšší částky, jež by přesáhla hranici, po jejímž dovršení či překročení se již výše uváděná daň platit nemusí. V tomto případě již skutečně většina obětí celou věc oznámí. V jednání pachatele je patrná jeho příprava, často počítá mimo jiné například s možností, že oběť nemá vozidlo a nemá se k bitcoinmatu nebo do své banky v co nejkratší době jak dostat. Z tohoto důvodu jí útočník třeba prostřednictvím internetu zajistí taxi službu, kdy s obětí celou dobu telefonuje a sděluje jí, aby si uschovala účtenku od taxikáře, protože jí tuto taxu banka následně proplatí. Ze začátku se uvedení útočníci zaměřovali především na občany států východní Evropy žijících v České republice, následně se však rovněž přeorientovali na občany České republiky.[30] [31]

Útoky „Ruský bankéř“ se v průběhu času vyvíjely a taktéž měnily, v nedávné minulosti již útočníci hovořili plynule českým jazykem, současně měnili svůj postup, kdy nejdříve chtěli jen nabourat internetové bankovnictví a získat do něj

---

[30] JANČOVÁ, Andrea. A11 S.R.O. *Další podvod na klienty bank! Tentokrát se ozývá fiktivní ruský bankéř.* Online. Dostupné také z: https://nasregion.cz/dalsi-podvod-na-klienty-bank-tentokrat-se-ozyva-fiktivni-rusky-banker- 255244/?utm_source=www.seznam.cz&utm_medium=sekce-z-internetu. [citováno 2024-02-09].

[31] NEUBAUEROVÁ, Tereza. POLICIE ČESKÉ REPUBLIKY -TÝDENÍK POLICIE. *Rusky mluvící falešný bankéř se zaměřuje na Ukrajince a Rusy žijící v České republice*. Online. Dostupné také z: https://tydenikpolicie.cz/rusky-mluvici-falesny-banker-se-zameruje-na-ukrajince-a-rusy-zijici-v-ceske-republice/. [citováno 2024-02-09].

přístup od oběti, následně však celou věc zdokonalili a propracovali výše uvedeným způsobem.

5 Legislativa a právní kvalifikace skutků

J. Kolouch a P. Bašta uvádějí: *„Zejména díky specifičnosti spočívající v neohraničenosti kyberprostoru a potřebě účinné mezinárodní spolupráce se EU snaží sblížit právní úpravu jednotlivých členských států tak, aby bylo možné efektivně řešit problematiku kybernetické bezpečnosti.“*[32]

Legislativou pro prověřování uvedených podvodných útoků je mnoho, je důležité vědět, že Česká republika je součástí Evropy a Evropské unie, a proto legislativa obsahuje i velké množství legislativy právě z Evropské unie, právní úprava Evropské unie slouží k propojení a srovnání právních úprav pro řešení kybernetické bezpečnosti všech členských zemí Evropské unie.

Primárním právem Evropské unie je Listina základních práv Evropské unie a dále směrnice, nařízení rozhodnutí a další dokumenty.[33]

Pro právní kvalifikaci podvodných investic jsou ale důležité právní normy České republiky, především se útočnici dopouští následujících trestných činů: podvod podle § 209, legalizace výnosů z trestné činnosti podle § 216, neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací podle § 230, opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231, neoprávněné opatření, padělání a pozměnění platebního prostředku podle § 234. Vše dle zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

Avšak i oběti se mohou dopouštět nedbalostních trestných činů, a to legalizace výnosů z trestné činnosti z nedbalosti podle § 217, neoprávněný zásah do počítačového systému nebo nosiče informací z nedbalosti podle § 232, obojí dle zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

---

[32] KOLOUCH, J. a BAŠTA, P. *CyberSecurity. 1. vydání.* Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-8. str. 95. [citováno 2024-02-09].
[33] KOLOUCH, J. a BAŠTA, P. *CyberSecurity. 1. vydání*. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-8. str. 96. [citováno 2024-02-09].

Pro prověřování podvodných investic se policejní orgán musí řídit platnou legislativou a postupovat podle zákona č. 141/1961 Sb., Zákon o trestním řízení soudním (trestní řád), případně postupovat podle zákona č. 273/2008 Sb., Zákon o Policii České republiky.

6 Příjem oznámení – výslech oběti podvodných investic

Výslechem oběti rozumíme prvotní výslech při prvotním podání oznámení obětí podvodných investic. Je tím myšleno jak podání vysvětlení dle § 61 zákona č. 273/2008 Sb., Zákon o Policii České republiky, ale především podání vysvětlení dle § 158 zákona č. 141/1961 Sb. Zákon o trestním řízení soudním (trestní řád).

Z autorových zkušeností vyplývá, že je v podáním vysvětlení oběti důležité především zjistit, na jakou nabídku investování do kryptoměn či jiných komodit oběť reagovala, kde byla nabídka zveřejněna, jak zněla a zda obsahovala nějaký obrázek (ten popsat). Na jaké stránky byla oběť přesměrována po otevření inzerátu, co se nacházelo na uvedených stránkách a zda jsou tyto stále aktivní (pro účely možného zablokování stránek přes portál CZ.NIC, který je správcem domén pro Českou republiku).

Dále je nezbytné zjistit, zda má oběť zálohovanou podobu stránek nebo odkaz na ně, jaké konkrétní údaje oběť vyplnila na stránkách, jak a kdy byla následně kontaktována. Pokud došlo k telefonickému kontaktu, z jakých telefonních čísel to bylo, dále informace k hovoru jako takovému, jak se volající osoba představila, jak hovor probíhal a co bylo obsahem, jakým jazykem (včetně přízvuku) osoba hovořila, zda má oběť záznam hovoru, na jaké telefonní číslo bylo oběti voláno, zda oběť volala na telefonní čísla zpět a s jakým výsledkem.

V dalších otázkách je třeba zaměřit se na zjištění, zda bylo po oběti vyžadováno uhrazení vstupního poplatku, v jaké měně, na jaký bankovní účet, z jakého bankovního účtu tyto odeslala, z jaké platební karty či jiné platební platformy byly platby učiněny, zda investované finanční prostředky byly majetkem oběti, nebo svěřené ke správě, půjčené, případně od koho, zda byla oběť vyzvána k instalaci aplikací pro vzdálené ovládání zařízení, pokud ano, do jakého zařízení a o jaké aplikace se jednalo. Jak byla instalace aplikace oběti zdůvodněna, odkud byla aplikace stažena, jak s aplikací oběť pracovala.

Policejní orgán dále u oběti ověřuje, zda došlo k dálkovému přístupu cizí osoby do jejího zařízení, jak konkrétně jej mohla cizí osoba ovládat, co bylo v zařízení za pomocí aplikace přesně prováděno. Oběť též uvede, zda se během doby, kdy bylo

její zařízení ovládáno jinou osobou přihlašovala do internetového bankovnictví, případně jiných internetových služeb.

Je třeba též zjistit, zda byla oběť vyzvána osobou, aby se do svého internetového bankovnictví přihlásila a jak tento krok osoba zdůvodnila. Oběť též popíše způsob, jakým se přihlašuje do svého internetového bankovnictví, přes jaké internetové stránky, případně pomocí jaké aplikace.

Oběť také uvede, zda osobě sdělila volající osobě své přihlašovací údaje do těchto aplikací a internetového bankovnictví a jaké úkony byly prováděny v jejím internetovém bankovnictví – kdo a jak přesně tyto prováděl, zda s úkony, které osoba v bankovnictví prováděla, oběť souhlasila, zda je musela schvalovat, a pokud ano, jak je schvalovala.

Nutné je též ověřit, zda bylo oběti známo, kam budou finanční prostředky převáděny, a pokud ano, zda s tím vyslovila souhlas. Oběť též sdělí, zda žádala v souvislosti s investováním o úvěr u banky či jiné instituce, v jaké výši, u jaké instituce a zda byl úvěr schválen. Pokud ano, jakým způsobem byly finanční prostředky z úvěru převedeny a kam, zda byl bez vědomí oběti učiněn pokus o získání úvěru v jejím internetovém bankovnictví, případně (bude-li tato informace oběti známa) jinde na její totožnost.

Oběť se dále vyjádří k otázce, zda byl pokus o získání úvěru úspěšný, kdy a jak se o této skutečnosti dozvěděla, u koho byly úvěry bez jejího vědomí vyžádány, v jakých výších, zda byly schváleny a kam byly finanční prostředky vyplaceny. Pokud byly bez vědomí oběti vyžádány úvěry, jaké další kroky v této věci učinila, s jakým výsledkem.

Velmi důležitá je rovněž informace, zda oběť zaznamenala z předmětné doby na svém bankovním účtu též příchozí platby, o kterých byla předem informována osobou, která s ní byla v kontaktu, pokud ano, jak byly platby zdůvodněny a jak bylo s nimi dále naloženo.

Oběť uvede, zda jsou jí známy osoby majitelů účtů, ze kterých finanční prostředky na její účet přišly a z jakého důvodu. Rovněž sdělí, na jaké investiční platformě (webové stránce) mělo proběhnout investování.

Ověří se také, zda má oběť do investiční platformy zřízen přístup a účet, zda má stále přístup.

Rovněž je důležité, aby oběť sdělila, zda viděla, že by se výše finančních prostředků, které byly převáděny z bankovního účtu oběti, promítla i v jejím účtu na investiční platformě. Pokud jsou finanční prostředky odeslané z jejího bankovního účtu zobrazené na účtu investiční platformy jako obchodované prostředky, na základě, čeho oběť nabyla dojmu, že je jedná o podvod.

Oběť také vypoví, zda se seznámila před založením účtu na investiční platformě s obchodními podmínkami.

Při příjmu oznámení oběť též podá informaci, zda zakládala účet na kryptoburze, zda prováděla registraci sama, nebo za pomocí jiné osoby a kde přesně účty zakládala.

Ověřuje se mimo jiné, zda má oběť do uvedených kryptoburz stále přístup, pokud ano, ať uvede, jaké transakce prováděla sama a jaké případně prováděla jiná osoba.

Nezbytné je i sdělení, zda oběť komunikovala s osobou pachatele i pomocí emailu, jestliže ano, nechť uvede jak svou emailovou adresu, tak emailovou adresu druhé osoby, ať uvede, o jaké zprávy šlo a co bylo jejich obsahem.

Prověří se také, zda bylo po oběti vyžadováno zasílání informací či dokumentů prostřednictvím emailu, a pokud ano, o jaké konkrétní dokumenty šlo, zda oběť druhé osobě poskytla své osobní doklady nebo jejich fotografie, kopie, jestliže ano, jakých a jak byla jejich potřeba zdůvodněna.

Nutné je rovněž zjištění, zda oběť s druhou osobou komunikovala i jiným způsobem, například s pomocí komunikačních aplikací, SMS zprávami a podobně, a pokud má jakoukoliv komunikaci, nebo jiné dokumenty k věci, zda je může pro účely vyšetřování poskytnout a předložit.

Dále je samozřejmě třeba výpověď oběti doplnit o otázky vyplývající z výše uvedeného. Na základě výslechu je možné dále postupovat v prověřování věci.

7 Příjem oznámení – výslech oběti vishingu („Ruský bankéř“)

V tomto případě výslechem oběti rozumíme prvotní výslech při prvotním podání oznámení obětí vishingu, především oběti podvodu „Ruský bankéř“. Je tím myšleno jednak podání vysvětlení dle § 61 zákona č. 273/2008 Sb., Zákon o Policii České republiky, ale především pak podání vysvětlení dle § 158 zákona č. 141/1961 Sb. Zákon o trestním řízení soudním (trestní řád).

Výslech je obdobný tomu, který byl uveden výše v bodě „Příjem oznámení – výslech oběti podvodných investic.“

Dále je třeba zaměřit se na další aspekty, a to především:

- jakým způsobem a jak konkrétně byla oběť útočníkem instruována k provedení výběrů finančních prostředků nebo zaslání transakcí ze svých účtu

- na jakých místech měla oběť učinit výběry a vklady hotovosti, přesnou lokaci bankomatů (i bitcoinmatů), tj. adresa, příp. obchodní dům (název, bližší určení polohy atd.)

- zda se oběť na místo popsané v předešlém bodě přepravovala sama, pokud ne, jakým způsobem, tj. uvést název přepravce, taxislužby, a to včetně telefonního čísla a dalších upřesňujících údajů

- zda má oběť nějakým způsobem zálohovanou i uchovanou komunikaci z komunikačních aplikací, pokud ano, vyzvat oběť k jejímu vydání, dále pak ke sdělení legendy, pod níž byla útočníkem ke svému jednání přesvědčena

- zda má oběť hlasovou nahrávku hovoru, případně zda je možné tuto vydat policejnímu orgánu a dále ji zajistit jakožto důkazní materiál

- zda je útočník stále v komunikačním spojení s obětí, nebo zda již komunikace skončila

- jestliže nebyla obětí pořízena hlasová nahrávka hovoru s útočníkem/útočníky, je třeba se jí dotázat na jméno a příjmení, kterým se útočník, případně útočníci (bylo-li jich více) oběti představili, zda bylo oběti sděleno, odkud hovor probíhá, dotázat

se dále oběti na intonaci a přízvuk hlasu volajícího/volajících, případné výslovnostní či gramatické odchylky od normy atd.

Je třeba se zaměřit se také na zjištění, jaké informace o oběti již útočníci dopředu měli a jaké jim oběť sdělila až v průběhu vlastního hovoru. Toto obvykle bývá jedna z nejsložitějších částí výslechu, neboť oběť je ovlivněna manipulativním jednáním útočníků, kteří v ní vyvolají mylné zdání, že veškeré informace o ní již má, ačkoliv je reálně získává právě až během hovoru s obětí.

8 Neodkladné a neopakovatelné úkony

Prvotní úkony ve věci, mezi něž patří i neodkladné a neopakovatelné úkony, zpravidla provádí, samozřejmě s přihlédnutím na právní kvalifikaci skutku, útvar, který oznámení přijímá. Vzhledem k zatíženosti útvarů Služby kriminální policie a vyšetřování přebírají dost často prvotní úkony základní organizační články, tedy obvodní a místní oddělení Policie České republiky.

Vzhledem k problematice jednotlivých podvodných útoků v informačních a komunikačních technologiích je třeba zaměřit se již při příjmu oznámení s ohledem pro následné prověřování právě na neodkladné a neopakovatelné úkony.[34]

Na základě výše popsaných skutečností je tedy zcela zřejmé, že je nutné již při samotném příjmu oznámení brát nejvyšší zřetel na získání co největšího možného množství relevantních informací zjištěných od oznamovatele či poškozené osoby. Dále je třeba se zaměřit na napadenou výpočetní techniku (stolní počítač, notebook, mobilní telefon aj.), v uvedených elektronických zařízeních oběti je třeba zaměřit se na veškerá data, spojená s útokem jako takovým, tj. od základní komunikace s pachatelem prostřednictvím SMS zpráv a telefonních hovorů, až po komunikaci uskutečněnou přes různé aplikace, jež byly uvedeny v popisné části této práce (Facebook messenger, Whatsapp, Telegram, Viber, aj.).

Komunikace vedené na těchto aplikacích lze uložit do zařízení a zaslat emailem nebo je přesunout přes externí hardware (flashdisk, přenosný HDD a podobně) do policejních systémů ke spisovému materiálu jako data, případně je samozřejmě možné uložit tato data na CD, DVD nosič, který bude taktéž přiložen jako součást spisového materiálu. Komunikace je následně vyhodnocována především pro zjištění přesného modu operandi pachatele, neboť z komunikace lze vyčíst větší část nebo celý průběh jednání pachatele. To je pro ucelený pohled na skutek jako takový velmi důležitý aspekt a je to taktéž velmi důležité pro stanovení právní kvalifikace skutku. Z jednotlivých komunikací lze vyčíst klíč a postup, kterým pachatel jedná, zejména jakým způsobem vede poškozeného k tomu, aby vzbudil jeho

---

[34] *Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)* v posledním znění.

důvěru, jakou záminku (legendu) pro vylákání finančních prostředků užil a taktéž jakým způsobem zajistil převod finančních prostředků oběti a kam. Právě zmíněné informace jsou stěžejní pro následný postup policejního orgánu při zajišťování vylákaných finančních prostředků. Velmi důležité při analýze těchto komunikací je též zjištění platformy užité pachatelem s přihlédnutím k možnostem jejího užívání, např. údaj o tom, zda se pachatel musí do platformy zaregistrovat a konkrétním jakým způsobem.

Ve věci zajištění veškerých souborů ke spisovému materiálu je nutná součinnost s majitelem uvedených dat, které cílí k provedení následného řádného zapečetění zajištěných dat – tato stažená data jsou tedy opatřena kontrolní sumou v aplikacích Wincomander, Igorware hasher, Multihasher, nebo Hashmyfiles, případně v jiných podobných aplikacích, které vytváří nezaměnitelný kód HASH, ve výstupu MD5, SHA1, CRC32 a podobně, kdy výstupy se liší počtem znaků, čímž stoupá i bezpečnost ověření. Hash je výsledkem hashovacích algoritmů/funkcí, je to matematická operace, která změní vložená data na kód tvořený číslicemi a písmeny určité délky (právě dle výstupu MD5, SHA1 a podobně). Jedná se o nezaměnitelný kód, tedy jasný identifikátor dat. Uvedený kód se zapisuje i do protokolu o ohledání předloženého zařízení, aby bylo zřejmé, že při ohledání věci byla zajištěna přesně tato data, jelikož při jakékoliv změně dat, přepsání či editaci, se změní taktéž kontrolní kód HASH, čímž dojde k zjištění, že data byla změněna, zaměněna.

V aplikacích Facebook messenger, Instagram, Snapchat a jím obdobným aplikacím, se jedná o přístup pomocí účtu na uvedených sociálních sítích či případně přímo zaregistrováním v aplikaci, a to pomocí emailové schránky, přes níž je třeba registraci potvrdit. Je tedy zřejmé, že v tomto případě je užito minimálně emailové schránky, jíž lze k případu za určitých podmínek zjistit od společnosti Meta Platforms. Z emailové schránky a taktéž od společnosti Meta Platforms, je možné získat informace k IP adresám osoby, která na emailovou schránku a taktéž Facebook messenger přistupovala.

K pachateli je tedy možné získat informace ze samotné komunikace, ale taktéž z emailové schránky a dále zjištěné IP adresy.

Do aplikací Whatsapp, Telegram, VIber a jím podobným aplikacím se přístup získává zaregistrováním telefonního čísla, tedy volající osoba (útočník) musí disponovat reálným telefonním číslem, jež by mělo být aktivováno a vloženo v nějakém zařízení. Z výše uvedeného vyplývá, že je zejména důležité zaměřit se na tuto skutečnost, tedy provádět šetření k telefonnímu číslu volajícího: u jakého operátora je vedeno, jaké zde figuruje předčíslí (kód země, v níž bylo telefonní číslo zakoupeno), zda se jedná o předplacenou službu (tedy způsob dobíjení kreditu v mobilním telefonu) nebo o službu paušální. V tomto případě je nutné zaměřit se na osobu majitele paušální služby, neboť tato osoba musela tuto komunikační aplikaci aktivovat, buď pro sebe, nebo musela být v kontaktu s osobou, pro níž tuto aktivaci učinila. Je třeba si rovněž uvědomit, že předplacené SIM karty je možné zakoupit anonymně, tedy není možné zjistit osobu držitele SIM karty, na kterou je vázán tento druh komunikační aplikace. Ovšem mimo informací vyplývajících přímo z komunikace, zde nadále existuje možnost zjistit IP adresy, ze nichž se pachatel do komunikačních aplikací připojoval. K pachateli je tedy možné získat informace ze samotné komunikace, ale taktéž z telefonního čísla a dále identifikované IP adresy.

Komunikace nesčetněkrát probíhá také prostřednictvím emailové komunikace. Každá emailová zpráva se skládá z tzv. hlavičky, tuto si lze představit jako ekvivalent poštovní obálky – je strukturovaná do řádků obsahujících informace o odesílateli, příjemci, předmětu zprávy, datu, IP adrese pisatele zprávy a podobně. Je třeba si uvědomit, že podrobná emailová hlavička je pro běžného uživatele skrytá, ve zprávě se ukazuje pouze velmi zredukovaná podoba hlavičky (záhlaví zprávy). Záhlaví zprávy, lze zfalšovat, pozměnění údajů v hlavičce je výrazně těžší a některé části hlavičky není možno zfalšovat vůbec. Dále se pak emailová zpráva skládá z těla zprávy, zde se jedná o vlastní obsah zprávy, tedy text a případné přílohy.

Zajištění emailového souboru, je třeba činit tak, aby byl použitelný jako důkaz. Soubor obsahuje původní zprávu i s připojenými soubory a taktéž kompletní emailovou hlavičku, většinou jde o soubory s koncovkou .eml nebo .msg spustitelné v programu Outlook nebo v programu Thunderbird, je zřejmé, že co poštovní

klient, to jiný způsob stažení souboru. U některých klientů nelze stáhnout více zpráv najednou. Proto je dobré k tomuto účelu využívat program Thunderbird.

Pro další prověřování je tedy zjevně důležité zajištění hlavičky emailu, což je protokol ve formě prostého textu, který obsahuje informace o tom, co se s emailem děje od jeho vytvoření až po jeho doručení. Je to jakýsi „životopis“ emailu.

Nemá žádný pevný databázový formát, ale běžně zde najdeme níže uvedené řádky:

from(odesílatel), to (adresát), subjekt (předmět), date (datum), return path (kam vracet v případě problémů), reply-to (na jakou emailovou adresu odeslat odpověď), date (časové razítko), ID (jedinečný kód, který je vygenerovaný při prvním vytvoření zprávy), recieved (jednotlivé položky identifikující systémy přes které email prošel – jako první je cílová stanice, poslední je zdrojová stanice). Zcela důvěryhodný zápis je pouze ten, který vytvořil váš mail server nebo váš počítač, nicméně důvěřovat lze i řádkům recieved, kde hledáme zápis poštovního serveru odesílatele. Při čtení hlavičky se nejprve sleduje první zápis, tj. recieved, odspodu.

Z výše uvedeného vyplývá, že k pachateli lze získat informace jak ze samotné komunikace, ale taktéž ze zjištěné IP adresy, domény a emailu.

K emailovým schránkám lze získávat informace na základě různých ustanovení trestního řádu, k základním informacím lze užít ustanovení § 8 odst. 1 trestního řádu, které policejní orgán opravňuje zjišťovat logy přístupu do emailové schránky, mimo soukromých údajů lze též zjistit údaje identifikační a registrační (alias, datum založení schránky, využití kapacity, počet zpráv, počet kontaktů, počet čísel mobilních telefonů), datum a čas posledního přijatého a odeslaného emailu, informace zda byl využit institut zapomenuté heslo, vyhledání všech účtů určitého uživatele, informace o všech službách využitých uživatelem, provedení zálohy obsahu schránky pro účely pozdějšího vydání na základě příslušného soudního rozhodnutí.[35]

---

[35] Zákon č. 141/1961 Sb., *o trestním řízení soudním (trestní řád)* v posledním znění.

K dalšímu vyžadování informací je, s přihlédnutím k právní kvalifikaci konkrétního skutku, třeba využít ustanovení § 88 trestního řádu, kterým lze v reálném čase provádět odposlech a záznam zpráv, jakožto i zpráv do budoucna.[36]

Ustanovení § 88a trestního řádu umožnuje prolomení zvláštní povinnosti mlčenlivosti uložené povinným subjektům zákonem č. 127/2005 Sbírky o elektronických komunikacích.[37]

Ustanovení dle § 158d odst. 3 trestního řádu slouží k povolení pro vstup do uzavřených prostor (možno chápat i do emailové schránky), zde můžeme zjistit obsah schránky včetně obsahu uložených zpráv, kdy pro policejní orgán není rozhodující, zda je emailová zpráva označena jako přečtená či nikoli (jelikož si ji může uživatel označit jako nepřečtenou i po jejím přečtení). Rozhodující je skutečnost, zda adresát zprávy (uživatel emailové schránky) měl objektivní možnosti zprávu přečíst. Lze zjistit kontakty z adresáře, telefonních čísel spojených se schránkou, smluvní ujednání a podobně.[38]

V rámci šetření (před zahájením úkonů trestního řízení) lze používat § 18 zákona č. 273/2008 Sbírky, o Policii České republiky, případně taktéž § 66 nebo § 68 zákona č. 273/2008 Sbírky, o Policii ČR.[39]

Z komunikací s pachatelem je velmi důležité zajistit informace k trase vylákaných finančních prostředků, kdy pachatel musí poškozenému sdělit jakým způsobem a kam má finanční prostředky zaslat, ve většině případů se setkáme s číslem bankovního účtu (ať v České republice, či zahraničí), dále se můžeme setkat s číslem kryptopeněženky, nebo dalšími účty u bankovních společností typu Revolut, WesternUnion a podobně.

V mnoha případech pachatel přemluví poškozenou osobu, aby do svého zařízení nainstalovala aplikaci třetí strany, v tomto případě se práce zaměřuje na programy pro vzdálený přístup do zařízení, programy umožňují vzdálený přístup, mohou

---

[36] Zákon č. 141/1961 Sb., *o trestním řízení soudním (trestní řád)* v posledním znění.
[37] Zákon č. 141/1961 Sb., *o trestním řízení soudním (trestní řád)* v posledním znění.
[38] Zákon č. 141/1961 Sb., *o trestním řízení soudním (trestní řád)* v posledním znění.
[39] Zákon č. 273/2008 Sb., *o Policii České republiky* v posledním znění.

být velmi užitečným nástrojem, ale zároveň i velmi nebezpečným nástrojem četně využívaným podvodníky pro spáchání různých podvodů. Těchto nástrojů je velké množství (AnyDesk, TeamViewer, SupRemo a podobně). Připojením se prostřednictvím těchto nástrojů získává pachatel vzdálený přístup do zařízení poškozeného, zde pak dochází k zneužití uvedených programů pro vzdálený přístup, kdy pod záminkou (legendou) výhodných investic a podobně přichází pachatel s nabídkou technické podpory a pomoci oběti, toto jednání pachatele pak většinou vyústí v ovládání finančních prostředků na účtu oběti.

Při prověřování uvedených podvodných útoků je třeba zajistit data z uvedených nástrojů nainstalovaných v zařízení poškozeného, protože je reálně možné z těchto dat získat IP adresu pachatele, případně údaje o zařízení, z nějž pachatel přistupoval vzdáleným přístupem do zařízení poškozeného. Ve většině případů se zajištěná data zajišťují během ohledání zařízení a jsou tak zajištěna jako důkazní prostředek ke spisovému materiálu.

8.1 Prolomení bankovního tajemství

Policejní orgán je povinen již při příjmu oznámení zjistil od poškozené osoby číslo bankovního účtu, z nějž byly pachateli zaslány finanční prostředky. Pro další potřeby prověřování věci je třeba od poškozeného neprodleně zajistit souhlas s poskytnutím informací, na které se vztahuje bankovní tajemství, podle § 38 a násl. zákona číslo 21/1992 Sb., o bankách. Tento souhlas je třeba vyžádat jak k bankovním účtům poškozené osoby, tak i k platebním kartám k předmětným účtům připojených.

Souhlas je poskytnut výlučně pro potřeby orgánů činných v trestním řízení k určitému číslu jednacímu a údaje takto získané nelze využít pro jiný účel než pro trestní řízení, v jehož rámci byly vyžádány. Pro účely trestního řízení ve věci je třeba zajistit údaje jen v takovém množství, v jakém jsou potřeba.

V případě, že svůj bankovní účet obsluhoval poškozený sám, není třeba, aby byly zajišťovány IP adresy přístupů do bankovního účtu. Pokud s bankovním účtem oběti manipuloval pachatel, ovšem nikoliv prostřednictvím programu pro vzdálené

ovládání ze zařízení poškozeného, jsou naopak IP adresy pro trestní řízení důležité. Nezbytnou nutností, která tomuto předchází, je samozřejmě zajištění výpisu z bankovního účtu oběti s přesnými údaji o datech a časech, kdy docházelo k podvodnému útoku.

Z výpisu vyžádaného od banky, kde má oběť veden svůj účet /účty, je tedy možné získat IP adresy osoby, která k bankovnímu účtu přistupovala, informace o tom, zda došlo k použití, resp. zneužití platební karty v rámci mobilního telefonu a čipu NFC. Údajů o provedené tokenizaci platební karty s uvedením data jejího provedení, názvu zařízení či aplikace a všech ID údajů spojených s tokenizací a identifikací zařízení (jako je IMEI), identifikace čísla dotazované platební karty oprávněného držitele, přehled použití platební karty, místo, datum, čas, druh transakce, výše požadovaných i schválených částek, identifikace bankovního účtu majitele, oznamovatele (číslo, datum založení, dispoziční práva, příp. další skutečnosti), řádný výpis z bankovního účtu a to jak schválených i neschválených plateb, případně dalších skutečností k bankovnímu účtu dle typu prověřované věci. Získané informace jsou pro policejní orgán důležité zejména z toho důvodu, že po zjištění příjemce finančních prostředků je možné následně přistoupit k úkonu zajištění finančních prostředků, tj. k jejich blokování na cílovém bankovním účtu, a taktéž je tímto způsobem možné zjistit totožnost majitele cílového bankovního účtu s využitím ustanovení § 8 odst. 2 trestního řádu.[40]

8.2 Prolomení údajů o telekomunikačním provozu

Pokud poškozený s pachatelem komunikoval i za využití mobilního telefonu prostřednictvím telefonického hovoru, je třeba od poškozeného zjistit konkrétní účastnická čísla těchto hovorů – zjišťuje se tedy jak telefonní číslo poškozeného, tak telefonní číslo/čísla pachatele. Z toho důvodu je třeba od poškozeného zajistit souhlas k poskytnutí údajů o uskutečněném telekomunikačním provozu podle § 88a odst. 4 trestního řádu. Souhlas může dát každý uživatel účastnického čísla anebo

---

[40] Zákon č. 141/1961 Sb., *o trestním řízení soudním (trestní řád)* v posledním znění.

jeho zákonný zástupce. Souhlas je poskytnut výlučně pro potřeby orgánů činných v trestním řízení k určitému číslu jednacímu a údaje takto získané nelze využít pro jiný účel než pro trestní řízení, v jehož rámci byly vyžádány. Pro účely trestního řízení ve věci je třeba zajistit údaje jen v takovém množství, v jakém jsou potřeba. Tedy se souhlas uděluje na určité období. Následným sdělením od telekomunikační společnosti je možné ověřit telefonní čísla, ze kterých pachatel poškozenému telefonoval.[41] Z vyžádaného výpisu o uskutečněném telekomunikačním provozu je možné ověřit možnost spoofingu, případně i zjistit majitele telefonního čísla, z nějž pachatel telefonoval.

8.3 Zajištění finančních prostředků

Z výslechu poškozeného, zajištěné komunikace s pachatelem, a zejména pak z vyžádaného bankovního účtu poškozeného, jsou zjištěny informace k bankovnímu účtu, kam poškozený na pokyn pachatele pod určitými legendami zaslal své finanční prostředky. Pokud poškozený neposkytne policejnímu orgánu výše popsaný souhlas s poskytnutím informací, na které se vztahuje bankovní tajemství, podle § 38 a násl. zákona číslo 21/1992 Sb., o bankách, případně není možné tento souhlas získat, je možné výpis z bankovního účtu zajistit na základě ustanovení § 8 odst. 2 trestního řádu. Následně je třeba, aby policejní orgán velmi rychle jednal a pokusil se v souladu s § 79a odst.1 trestního řádu zajistit finanční prostředky oběti jakožto výnos z trestné činnosti. Pro policejní orgán je v této chvíli důležitý především čas, neboť věc nesnese odkladu, a to z důvodu možného přečerpání finančních prostředků na jiné účty, možného fyzického výběru finančních prostředků či jejich vyvedení mimo Českou republiku do zahraničí. O výše uvedeném úkonu zajištění peněžních prostředků sepíše policejní orgán Usnesení podle § 79a odst. 1 trestního řádu ve dvou formách, a to zkrácené usnesení bez odůvodnění a usnesení s odůvodněním.

---

[41] Zákon č. 141/1961 Sb., *o trestním řízení soudním (trestní řád)* v posledním znění.

Zkrácené usnesení o zajištění bez odůvodnění se zasílá například bance nebo katastrálnímu úřadu. Usnesení o zajištění s odůvodněním se zasílá až následně po provedení zajištění, například obviněné osobě. Po formální stránce se jedná o dvě samostatné písemnosti. To znamená, že v rámci obsahu spisu budou vedena tato usnesení dvě, a to s různými pořadovými čísly). V jednotlivých usneseních je třeba řádně definovat, zda se jedná o zajištění po předchozím souhlasu státního zástupce či nikoliv Pokud byl předchozí souhlas státního zástupce k předmětnému úkonu udělen, uvádí se v usnesení jméno a příjmení státního zástupce, datum vydání jeho souhlasu a spisová značka státního zastupitelství. Jestliže v naléhavém případě, který nesnesl odkladu k udělení předchozího souhlasu státního zástupce nedošlo, je třeba v usnesení rovněž uvést tuto skutečnost. Dále usnesení obsahuje informaci, u jaké společnosti je veden účet, na němž se zajištění uskuteční, přesné číslo dotčeného bankovního účtu, kód banky a především částka, kterou je třeba zajistit. Mohou se zajišťovat (a v praxi tomu tak většinou bývá) taktéž i peněžní prostředky dodatečně došlé na předmětný účet, včetně jejich příslušenství, a to až do určité odůvodněné hodnoty.

Uvedené skutečnosti je třeba v odůvodnění řádně odůvodnit. Usnesení se následně zasílá na příslušné státní zastupitelství, cílové bance, osobě majitele bankovního účtu a zakládá se do spisu. Při vydání usnesení bez předchozího souhlasu státního zástupce je policejní orgán povinen své rozhodnutí předložit do 48 hodin státnímu zástupci, který s ním vysloví dodatečný souhlas, nebo jej zruší.[42]

Text poučení*: „Proti tomuto usnesení je přípustná stížnost, která se podává prostřednictvím vydávající součásti Policie České republiky dozorujícímu státnímu zástupci nejpozději do tří dnů od doručení tohoto usnesení. Stížnost nemá odkladný účinek a rozhoduje o ní soud, v jehož obvodu je činný státní zástupce, který ve věci vykonává dozor nad zachováním zákonnosti v přípravném řízení (§ 146a odst. 2 trestního řádu). Majitel cílového bankovního účtu má právo, kdykoliv po právní moci usnesení o zajištění, žádat o zrušení nebo omezení zajištění. Byla-li*

---

[42] Zákon č. 141/1961 Sb., *o trestním řízení soudním (trestní řád)* v posledním znění.

žádost zamítnuta, může ji, neuvede-li v ní nové důvody, podat znovu až po uplynutí 30 dnů od právní moci rozhodnutí, kterým bylo rozhodnuto o přechozí žádosti.

Se zajištěním věci jsou spojeny právní účinky. Právní jednání učiněné osobou, vůči níž směřují zákazy uvedené v rozhodnutí o zajištění, v rozporu se zákazy v něm uvedenými, je neplatné. Soud k neplatnosti přihlédne i bez návrhu. S věcí, na kterou se vztahuje rozhodnutí o zajištění, lze v rámci výkonu rozhodnutí, veřejné dražby, exekuce nebo insolvenčního řízení nakládat jen po předchozím souhlasu předsedy senátu a v přípravném řízení státního zástupce. Na úhradu pohledávek, které jsou předmětem výkonu rozhodnutí, veřejné dražby, exekuce nebo insolvenčního řízení, se přednostně použije věc nedotčená rozhodnutím o zajištění".[43]

8.4 Trasování Bitcoinu

Trasováním Bitcoinu se rozumí hledání trasy Bitcoinu cestou kryptopeněženek. Lze to chápat jako hledání cesty k cílové peněžence, ze které je následně Bitcoin opět přeměněn (prodán) za jinou měnu nebo na které je koncově uložen. Existují záznamy o všech transakcích s Bitcoiny. Bitcoin tedy není přímo anonymní měnou, jedná se spíše o pseudoanonymní měnu, což tedy v praxi znamená, že lze sledovat trasu Bitcoinu, ale adresa v bitcoinové síti není oficiálně spárována s osobou či organizací.

Bitcoinová adresa je identifikátorem v blockchainu, skládá se z 26-35 alfanumerických znaků s výjimkou znaku 0 (nula), O (velké o), I (velké i) a l (malé l). Z dostupných informací o množství toků Bitcoinů lze však identifikovat kryptopeněženky, které jsou součástí kryptoburz. Aplikací pro trasování Bitcoinu je velké množství, zde se zaměříme především na aplikace využívané policejními orgány.

---

[43] MOJŽÍŠ, Jiří. POLICIE ČESKÉ REPUBLIKY. *Usnesení podle § 79a odst. 1 trestního řádu.* Online. Dostupné také z: https://www.policie.cz/soubor/usneseni-o-zajisteni-veci-79a-odst-1-tr-r-ceska-sporitelna-a-s-pdf.aspx. [citováno 2024-02-09].

Proto budou níže vysvětleny jen jejich základní principy a dále uvedeno, kdo uvedené aplikace využívá.

8.4.1 Blockchain explorer

Blockchain explorery jsou jednou z nejzákladnějších veřejně dostupných možností k trasování. Jedná se o explorery (vyhledávače), jakými jsou například blockchain.com[44], walletexplorer.com[45], blockchair.com[46], www.btc.bitaps.com a další. Lze trasovat jen několik „kroků“ bitcoinu, neboť kvůli většímu množství dat nemusí být následně možné dohledat zbytek trasy. Uvedenou aplikací probíhá elementární trasování základními články Policie ČR, případně Oddělením analytiky a kybernetické kriminality, jež jsou součástí jednotlivých územních odborů.

8.4.2 Forensis od společnosti Elliptic

Aplikace Forensis od společnosti Elliptic[47] je placený a hlavně přesnější nástroj pro trasování bitcoinů, kterou využívá Odbor kybernetické kriminality na úrovni Odboru kybernetické kriminality při krajských ředitelstvích policie.

8.4.3 Reactor

Reactor je nástrojem od společnosti Chainalysis[48], který využívají pouze útvary s celostátní působností, a to Národní centrála proti organizovanému zločinu SKPV a Národní centrála proti terorismu, extremismu a kybernetické kriminalitě SKPV.

---

[44] Blockchain. BLOCKCHAIN.COM. *Blockchain.com.* Online. Dostupné také z: https://www.blockchain.com/. [citováno 2024-02-09].
[45] WalletExplorer. CHAINALYSIS. *Walletexplorer.com.* Online. Dostupné také z: https://www.walletexplorer.com/. [citováno 2024-02-09].
[46] Blockchair. BLOCKCHAIR. *Blockchair.* Online. Dostupné také z: https://blockchair.com/. [citováno 2024-02-09].
[47] Elliptic.ELLIPTIC. *Forensis.* Online. Dostupné také z: https://www.elliptic.co/. [citováno 2024-02-09].
[48] Reactor. CHAINALYSIS. *Reactor.* Online. Dostupné také z: https://www.chainalysis.com/. [citováno 2024-02-09].

Jedná se o aplikaci s nejpřesnější analýzou Bitcoinových adres a tras, kdy výsledkem bývá i graf trasy.

8.5 Spoofing

Spoofing nebo „falšování“ je nedílnou součástí podvodných investic a dalších podvodů využívajících prvků sociálního inženýrství. S pomocí spoofingu se útočník snaží anonymizovat svou totožnost, nebo se vydává za někoho jiného, většinou za nějakou populární osobnost či všeobecně uznávanou autoritu. Útočník se mnohdy vydává dokonce za státní instituce, banky, renomované společnosti, konkrétní jedince, policisty, bankéře, bezpečnostní poradce a podobně.[49] Nejčastěji využívaným typem spoofingu je maskování telefonního čísla volajícího. Tímto maskováním rozumíme skutečnost, kdy osoba přijímací hovor na displeji svého zařízení vidí telefonní číslo organizace, jednotlivce, konkrétního regionu podle předvolby a podobně. Tedy se příjemci hovoru zobrazí jiné číslo než je to, z nějž útočník ve skutečnosti volá, zobrazují se tak telefonní čísla například bank, policistů a podobně. Slabinou telefonního spoofingu je ovšem fakt, že když příjemce hovoru zatelefonuje zpět volajícímu, dovolá se na skutečné telefonní číslo, použité útočníkem, tedy opravdu do některé banky, na některý z policejních útvarů atd. Stejným způsobem lze využít spoofing u konkrétní emailové adresy, webové stránky a jinde. V případě okamžitého prověřování policejním orgánem je od uskutečněného spoofovaného hovoru v řádu dnů, až měsíců (u každého operátora v České republice je tomu jinak) možné zjistit informace k subjektům, přes něž byl spoofovaný hovor veden. Například A1 Telecom Austria AG (Rakousko), Afinna One Srl Sole Shareholder (Itálie), Apelby GmbH (Německo), BT Global Europe B.V (sídlo v České republice), CETIN a.s. (Česká republika) a podobně. Záleží na tom, jak (popř. jakým způsobem a v jakém rozsahu), výše jmenované subjekty reagují na komunikaci s orgány činnými v trestním řízení. Některé bohužel nekomunikují vůbec. V případě řádně a včas podané žádosti policejním

---

[49] VOŘÍŠEK, Lukáš. INSMART. *Co je to spoofing?* Online. Dostupné také z: https://insmart.cz/co-je-spoofing/. [citováno 2024-02-09].

orgánem, lze však od některých z nich na základě doručené odpovědi zjistit informace i k reálným telefonním číslům, nebo zařízením, z nichž byl učiněn spoofovaný hovor.

8.6 Typy IP adres a možnosti jejich anonymizace

Typy IP adres můžeme dělit na adresy typu NAT, Proxy Servery a VPN.[50]

Při připojení se na NAT (například pomocí routeru v domácnosti) dojde k výměně IP adresy připojeného zařízení za IP adresu jinou, která komunikuje s veřejným internetem, jedná se tedy o oddělení vnitřní a veřejné sítě, což znamená, že může být do veřejného internetu připojeno mnoho zařízení (stovky) skrze jednu IP adresu. Tak fungují třeba mobilní operátoři. NAT sám o sobě není bezpečnostním prvkem. Cílem je úspora IP adres, anonymizace je vedlejším produktem.

Proxy skryje IP adresu před veřejnou sítí a vymění ji za IP adresu právě proxy serveru. Jedná se o nízkou úroveň anonymizace a ochrany soukromí na internetu, protože pracuje většinou pouze s webovým provozem a komunikace jako taková není nijak šifrovaná. Proxy servery jsou často využívané ve firmách, kde je důležitá bezpečnost, rychlost, usnadnění. Jde tedy o nižší stupeň anonymizace.

VPN, tedy Virtual Privat Network (Virtuální privátní sít) je velmi podobný typ jako Proxy, ale právě kromě skrytí IP adresy při prohlížení internetových stránek a webu jako takového, nabízí skrytí celkového internetového provozu, navíc se jedná o bezpečné šifrované spojení mezi zařízením a internetovou sítí. Právě VPN je často zneužívána pachateli k anonymizaci jejich jednání a útoků na internetu. VPN jako taková je nabízena mnoha společnostmi, jelikož anonymizační služby mohou být využity i jinak, než pro páchání internetových podvodů a útoku (za zmínku stojí například návštěva webových stránek, které nejsou v zemi dostupné). Přes VPN se tak můžeme k webovým stránkám připojit IP adresou i ze zcela jiné části planety. Jedná se o běžnou součást prohlížečů a antivirů,

---

[50] IP adresa. *Mojeip.cz.* Online. Dostupné z: https://www.mojeip.cz/. [citováno 2024-02-09].

protože zvyšuje bezpečnost soukromí za cenu pomalejšího připojení. Jde tedy o nejvyšší stupeň anonymizace, protože šifruje.

9 Prevence

9.1 Možnosti prevence útoků sociálního inženýrství

Základním předpokladem pro možnou prevenci útoků sociálního inženýrství je schopnost rozlišit, o jaký konkrétní typ útoku jde. Právě při prevenci je třeba apelovat na použití „zdravého selského rozumu“, kdy se potenciální oběť nesmí útočníkem při vzájemné komunikaci nechat, jakkoliv zastrašit, dostat se do subjektivně vnímané stresové situace časové tísně, či jiného submisivního postavení během hovoru. Je třeba připomínat podezíravost a obezřetnost, taktiku včasného „ne, nemám zájem“, možnost ukončení komunikace a následné blokace podezřelého telefonního čísla, emailu apod. Zvláštní důraz by měl být kladen i na upozornění neposkytovat osobní a citlivé informace ohledně své osoby a svého bankovnictví, nesdělovat a neposílat nikomu své citlivé informace včetně intimního obsahu. Ověřovat si, zda je v komunikaci využit správný komunikační prostředek a jeho kanál, tedy zda příjemce komunikuje skutečně s tím, s kým má, a to i přes skutečnost, že se zdánlivě jedná o správný informační kanál. Jak je výše popsáno, nemusí to vždy znamenat, že na druhé straně není pachatel útoku v kyberpeostoru. V tomto případě takzvaného spoofingu funguje jednoduché pravidlo, a to zavolat na telefonní číslo jevící se například jako reálné číslo banky zpět a ověřit si totožnost volajícího. Nezbytnou součástí se jeví též kontrola veřejně přístupných informací na sociálních sítích, zda z nich nelze zjistit informace, které by mohli pachateli výrazně pomoci cílit na potenciální oběti svůj útok (například různé osobní fotografie, příspěvky sdělující důvěrná sdělení o sobě, rodinných příslušnících, jejich fotografie atd). Pokud jednáme v internetovém prostředí a využíváme webových stránek k přístupu do různých aplikací, bankovnictví a podobně, je opravdu bezpodmínečně nutné ověřit si, zda se skutečně nalézáme na stránce, kterou chceme navštívit, neboť zde existuje reálná možnost, že se ocitneme na podvodných internetových stránkách, jež se mají totožný či téměř totožný vzhled jako stránky originální (např. stránky ČSOB, Komerční banky a jiné), ovšem figurují pod jiným odkazem, který je záměrně velmi podobný odkazu originálnímu. Velmi dobrý pro

trénink opatrnosti v internetovém prostředí je interaktivní test na portále www.kybertest.cz.[51]

9.2 Opatření pro společnost

Základním předpokladem pro boj proti výše popsané kriminalitě je prevence společnosti. Prevenci kriminality v tomto případě můžeme rozdělit na tři rozdílné způsoby, a to na sociální prevenci, situační prevenci a prevenci možností stát se obětí, tedy viktimnosti. Samostatným oddílem pak zůstává pomoc obětem trestných činů.

Sociální prevence v případě kybernetické kriminality jsou *„aktivity ovlivňující proces socializace a sociální integrace a aktivity zaměřené na změnu nepříznivých společenských a ekonomických podmínek, které jsou považovány za klíčové příčiny páchání trestné činnosti.“*[52] Prevenci kriminality se zaobírá celá webová stránka Ministerstva vnitra s názvem „Prevence se musí vyplatit“, kdy jedna ze sekcí webových stránek se zabývá především prevencí kybernetické kriminality.[53]

Situační prevence je v případě této kriminality velmi efektivní a je třeba jí hojně využívat, jelikož se jedná o využití již získaných poznatků o páchané kriminalitě. Zde můžeme uvést, že třeba k podvodným vishingovým útokům „Ruský bankéř“ docházelo taktéž za využití bitcoinmatů nacházejících se v obchodních centrech a velmi efektivně zapůsobila reklamní kampaň Policie České republiky.[54] Reklama jako varování před podvody se nacházela přímo vedle nebo byla dokonce nalepená na určitých zařízeních – bitcoinmatech, a to samozřejmě za součinnosti a souhlasu majitelů či provozovatelů uvedených bitcoinmatů. Varování ohledně

---

[51] KYBERTEST.CZ. Buďte na internetu v bezpečí. *Kybertest.cz.* Online. Dostupné z: https://www.kybertest.cz. [citováno 2024-02-09].
[52] MINISTERSTVO VNITRA. *Prevence kriminality.* Online. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/. [citováno 2024-02-09].
[53] MINISTERSTVO VNITRA. *Kyberkriminalita.* Online. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/. [citováno 2024-02-09].
[54] KROFTOVÁ, Hana. *NEBUĎ BIT - BUĎ IN - BITCOINMATY*. Online. Dostupné z: https://www.policie.cz/clanek/nebud-bit-bud-in-bitcoinmaty.aspx. [citováno 2024-02-09].

možných podvodných jednání si dokonce softwarově nahrávali majitelé uvedených bitcoinamtů i v zařízeních, kde jej musela osoba užívající bitcoinmat po přečtení potvrdil, před dalším pokračováním.

Útočníci využívají samozřejmě různé nástroje trestné činnosti, výjimečné není ani užití právě aplikací pro vzdálený přístup do zařízení, kdy třeba právě společnost AnyDesk jak v samotné aplikaci, tak i na svých internetových stránkách varuje uživatele aplikace proti podvodným jednáním.[55]

Stejně jako provozovatelé aplikací a zařízení k věci přistoupily bankovní společnosti, které ve svých internetových bankovnictvích, obrazovkách bankomatů, na svých webových domovských stránkách i jinde informují a varují své klienty před možnými podvody ze strany útočníků, a to opět i za spoluúčasti reklamy na internetu (YouTube, sociální síť Facebook a podobně) či v televizi. Velmi známou a úspěšnou kampaň má třeba Československá obchodní banka.[56]

Je tedy zřejmé, že i majitelé aplikací, zařízení i bank reagují na využívání jejich služeb pachateli trestné činnosti a za součinnosti Policie České republiky dělají vše proto, aby své uživatele chránili. Bylo by na místě, kdyby pomohla i legislativa, která by po vyhodnocení možných nástrojů využívaných útočníky uzákonila povinnost varování a výstrahy pro všechny uživatele, nejen v obchodních podmínkách, ale i na uživatelských rozhraních při používání jednotlivých zařízení a aplikací.

Pro prevenci viktimnosti je velmi důležité, aby se společnost vzdělávala v oblasti kybernetické bezpečnosti, a to formou různých přednášek, školení, případně za spoluúčasti Ministerstva školství, mládeže a tělovýchovy při zavedení kurzu základní bezpečnosti v kybernetickém prostoru, který by mohl být součástí některého z předmětů (informatika, občanská nauka atd.) již na základních a dále i středních školách. Většina dnešní nejmladší generace se totiž v internetovém prostředí pohybuje prakticky od dětství, děti od raného věku užívají mobilní

---

[55] ANYDESK. *How to Avoid Remote Access Scams*. Online. Dostupné z: https://anydesk.com/en/abuse-prevention. [citováno 2024-02-09].
[56] ČESKOSLOVENSKÁ OBCHODNÍ BANKA. *Braňte se rozumem.* Online. Dostupné z: https://www.csob.cz/branteserozumem. [citováno 2024-02-09].

telefony, mnohdy mají i bankovní účty, sdílejí své fotografie a důvěrné údaje na sociálních sítích – je tedy více než zřejmé, že právě děti a mládež mohou být snadným terčem různých útoků, jelikož on-line prostředí je pro ní běžnou součástí života.

Zároveň je ale třeba v oblasti kybernetické bezpečnosti vzdělávat i osoby středního a vyššího věku. Právě na tuto část populace prioritně cílí útoky sociálního inženýrství. Někteří lidé z této generační skupiny, zejména pak osoby věku vyššího, se v internetovém prostředí orientují zcela minimálně nebo jen částečně. Vývoj jednotlivých technologií se velmi rychle vyvíjí, mění a zdokonaluje. Osoby středního a vyššího věku často tyto změny nezaznamenávají a nemají šanci na ně nikterak reagovat – ať už z důvodu své zaneprázdněnosti, jisté dávky pohodlnosti či neochoty nebo již i pro pomalejší schopnost učení a chápání, počínající fyzická, a především psychická onemocnění (skleróza a jiné). Současně se ale tato část populace nadále snaží držet krok s dobou, tedy svět internetu zcela nezavrhují, nechávají jej na sebe působit, právě lidé z těchto generačních skupin nejčastěji chtějí investovat své našetřené peníze a tím je dále zhodnocovat, aby je mohli využít ve stáří nebo pro své děti, vnoučata a podobně. Právě z tohoto důvodu (předpoklad úspor) představují lidé středního a vyššího věku nejpočetnější část společnosti, na níž útočníci cílí. U značného množství případů dokonce přímo osoba středního či vyššího věku sama od sebe vyhledává v internetovém prostředí možnosti, jak s pomocí svých naspořených finančních prostředků vydělat další peníze, jak zbohatnout, investovat a podobně.

Zde se právě útočníkům velmi osvědčily již zmiňované cílené reklamy, uveřejněné například na sociálních sítích či ve webových prohlížečích. Tyto cílené reklamy se totiž přímo zaměřují na osoby vyhledávající možnosti investic. Bylo by více než žádoucí, kdyby ze strany majitelů a provozovatelů webových stránek, sociálních sítí a dalších platforem, kde se takové cílené podvodné reklamy nacházejí, byly prováděny důsledné kontroly nad zveřejňovaným obsahem. Obsah vyhodnocený jakožto podezřelý, by dále nebyl zveřejněn, a tím by byly před podvodnými útoky jednotliví návštěvníci internetového prostředí ochráněni.

Postačovalo by pouze, aby se reklama nekontrolovala až po jejím nahrání (což je výhodné pro majitele webových stránek, sociálních sítí, jelikož za reklamu dostanou předem zaplaceno) a zneužití, ale právě naopak ještě před tím, než bude na sociální sítě, nebo webové stránky umístěna. Bylo by vhodné, aby povinnost kontroly zveřejňovaného obsahu (i reklam), byla rovněž zakotvena v legislativě, a to včetně sankcí za nesprávné a nedostatečné provedení této kontroly. Samozřejmě je zřejmé, že by takový proces byl velmi obtížný, a to především k značnému množství reklamy na internetu, ovšem pokud si majitel webových stránek nechává za reklamu platit, měl by mít i povinnost kontrolovat její obsah před zveřejněním, nikoliv až po zjištění, že reklama je podvodná. V dnešní době kontrolu provádí umělá inteligence, která kontroluje pouze to, zda reklama neporušuje dobré mravy, nebo není závadná vzhledem k věku uživatelů pro jejich mravní vývoj, nepodporuje nenávist ke skupině obyvatel a podobně, ale neřeší obsah webových stránek ani zda se nejedná o podvodné stránky, které slouží k právě k dalším výše uvedeným podvodům.

Proto by bylo záhodno algoritmus umělé inteligence při kontrole reklamy více a technologicky dokonaleji vyvinout, případně upravit tak, aby byl kontrolován nejen zevnějšek reklam a webových stránek, na něž přesměrovává, ale taktéž jejich obsah a legálnost. V současné době si reklamu na sociálních sítích může prakticky zaplatit kdokoliv, aniž by prošel nějakou důslednější kontrolou totožnosti či kontrolou originality vkládaných dokladů, včetně jejich platnosti (viz zmínka v úvodu této práce). S postupným masívnějším nástupem umělé inteligence zahrnujícím též tvorbu obrázků, textů, videí atd., není problém vytvořit i falešné elektronické osobní doklady. Tyto jsou pak ze strany některých webových stránek, a dokonce i ze strany špatně zabezpečených zahraničních bankovních institucí přijímány jako pravé, což představuje ideální podhoubí pro nárůst internetové kriminality.

Zde je třeba se zaměřit na provozovatele a vývojáře umělé inteligence – pokud mají možnosti a práva vyvíjet takovéto aplikace, měli by mít i povinnost zajistit, aby nelegální doklady a obdobné dokumenty nebylo možné s pomocí umělé inteligence vytvořit. V zásadě je tedy třeba zaměřit při prevenci zrak společnosti na to,

aby tvůrce umělé inteligence měl za své dílo zodpovědnost, a především měl nad ním i plnou kontrolu. V případě porušování podmínek či zneužívání takových aplikací, by bylo společensky žádoucí, aby existovala možnost potrestat tvůrce a majitele aplikace, jež je zneužívána k páchání trestné činnosti, případně požadovat, aby majitel měl plnou zodpovědnost za ověřování a identifikaci osob využívajících uvedené aplikace, tedy aby policejnímu orgánu mohl po řádně odůvodněném dotazu dle platné legislativy sdělit, kdo využil jeho služeb k nelegální činnosti.

Takové možnosti jsou možné jen za předpokladu mezinárodní spolupráce napříč jednotlivými zeměmi. Rozhodně je třeba postupovat tak, aby vadné aplikace nebo ty, jež nelze nijak kontrolovat, bylo možno zrušit a smazat z dostupných zdrojů, zejména pak, aby bylo možné jejich výtvory identifikovat a rozpoznávat. Právě zde tkví další možnosti pro budoucí prevenci uvedené kriminality. Stejně jako se vytváří aplikace umělé inteligence pro páchání kriminality, zneužívání fotografií a videí pachateli, měla by společnost reagovat naopak tím, že budou vytvářeny aplikace, jež naopak vytvořený software umělou inteligencí budou umět rozpoznat.

Banky v České republice mají každá sama o sobě svoje vlastní bezpečnostní prvky a bezpečnostní opatření. Využitelnost a rozpoznatelnost podvodů je u bezpečnostních prvků jednotlivých bank na různých úrovních. Některé banky dokážou detekovat podezřelé bankovní účty, podezřelé transakce, kdy každá z bank na zjištění reaguje jiným způsobem – některé prostřednictvím svých operátorů volají klientovi a snaží se telefonicky klienta doptat na okolnosti zvláštních a neobvyklých plateb, případně jej varovat při podezření, že se stává obětí podvodného útoku, jiné mají pouze upozornění v internetovém bankovnictví. V tomto směru by banky měly daleko více spolupracovat na úrovni bezpečnosti mezi sebou, ačkoliv je jasné, že právě zabezpečení a bezpečnost jsou základními stavebními kameny tvořícími důvěryhodnost a spolehlivost banky, v minulosti to byl nejdůležitější ukazatel její kvality. V dnešní době má každá banka vlastní portfolio nabídek služeb a cílovou skupinu klientů, kdy součinnost v oblasti bezpečnosti bank a transakcí v České republice, by mohla zaštiťovat Česká národní banka. V současné době plní podobné úkoly Finanční analytický úřad, který se zabývá analytickou činností:

„Analytická činnost je základní a nejdůležitější činností FAÚ při plnění stěžejního úkolu, kterým je ochrana finančního systému České republiky před zneužitím k praní peněz a financování terorismu. FAÚ je v této oblasti plně zodpovědný za efektivní a funkční nastavení systému opatření proti legalizaci výnosů z trestné činnosti (AML – „anti-money laundering“) a proti financování terorismu (CTF – „counter terrorism financing“). Analytická činnost se odvíjí v rovině operativní a strategické. V rámci operativní analýzy probíhá příjem a analýza oznámení o podezřelých obchodech, na které navazuje distribuce výsledků analytických šetření příslušným orgánům veřejné moci. Strategická analýza představuje vyšší úroveň zobecnění zjištěných poznatků, analýzu trendů ML/TF a formulaci doporučení pro budoucí praktický či legislativní vývoj.“[57].

9.3 Opatření pro práci policejních orgánů

Jak je již výše uvedeno, prvotní úkony ve věci spáchání protiprávního jednání a jeho oznámení Policii České republiky zpravidla provádí (s přihlédnutím na právní kvalifikaci skutku) útvar, který toto oznámení přijímá. Vzhledem k zatíženosti útvarů Služby kriminální policie a vyšetřování přebírají dost často prvotní úkony obvodní a místní oddělení Policie České republiky. Policisté zařazeni na těchto organizačních článcích nemají ve většině případů zaměření na určitou problematiku trestné činnosti, jak tomu bývá na vyšších organizačních článcích Policie České republiky (např. SKPV: zaměření KYBER, zaměření DROGY a podobně), musí být univerzálními ve všech směrech. Nemohou tedy dopodrobna znát problematiku všech trestných činů, veškerou metodiku, všechny speciální úkony, jakými jsou například zajišťování dat, souborů, některé úkony nevykonávají vůbec, jelikož se jimi nezabývají s ohledem na své služební zařazení (např. znalecké posudky a jiné). Tento aspekt má velký zásah do efektivity prověřování a vyšetřování kybernetické trestné činnosti, jelikož mnohdy dochází k průtahům v trestním řízení, postupovaní spisů na nesprávné součásti Policie České

---

[57] FINANČNÍ ANALYTICKÝ ÚŘAD. *Analytická činnost*. Online. Dostupné z: https://fau.gov.cz/analyticka-cinnost#analyticka-cinnost. [citováno 2024-02-09].

republiky, přeslýchání poškozených osob, opakované zjišťování aktuálních informací a podobně. Výjimku netvoří ani absence úkonu zajišťování finančních prostředků či jiných dalších potřebných úkonů. Je tedy velmi důležité, aby se problematikou zaměřenou na tyto podvodné útoky zabýval (i v rámci základních útvarů Policie České republiky) speciálně proškolený policista s určitým zaměřením, znalostmi, vědomostmi v daném oboru, tento aspekt nesporně přispěje k výraznému zvýšení rychlosti a kvality dalšího prověřování a vyšetřování.

Pro práci policejních orgánů při prověřování podvodných útoků v komunikačních a informačních technologiích je velmi důležitá analýza a inovace během vyšetřování. Je zde důležité si uvědomit, že útočníci uvedených útoků jich páchají značné množství, jedná se tedy o organizovanou trestnou činnost, v níž je třeba legalizovat výnosy z této trestné činnosti. Zároveň pachatelé jdou skutečně s dobou, jsou vždy o několik kroků napřed před policejním orgánem. Pro úspěšné vyšetřování je důležité, aby se policisté vzdělávali v trendech kybernetické kriminality na školeních, která povedou profesionálové a znalci v uvedené problematice. Jen takto může dojít k předávání informací mezi policisty, a to i na nejnižší organizační články Policie České republiky, jelikož v mnoha případech se na prvotních úkonech podílí právě základní útvary Policie České republiky (obvodní a místní oddělení), případně až následně útvary územních odborů Služby kriminální policie a vyšetřování, či vyšších organizačních článků. K uvedeným školením je třeba uvést, že v současné době dochází k postupnému školení pracovníků Služby kriminální policie a vyšetřování, a to několikrát v roce v rámci IMZ (instrukčně metodického zaměstnání), aby následně mohli metodicky vést ostatní pracovníky na svých územních odborech a útvarech. Z tohoto důvodu taktéž vznikla na Krajském ředitelství policie Středočeského kraje pracovní skupina „Kyber“, v níž je autor bakalářské práce zařazen jako zpracovatel na Územním odboru Mladá Boleslav, kdy skupina má v rámci své činnosti přednostně zpracovávat kybernetickou trestnou činnost a taktéž se přednostně účastnit (s ohledem na kapacitu) školení IMZ, které probíhá taktéž formou videokonferencí v prostředí intranetu. Je zcela zřejmé, že policie směřuje dobrým směrem, ačkoliv se tyto projekty nacházejí pouze v prvotních fázích.

Analýzou kybernetické trestné činnosti se zabývají Odbory analytiky a kybernetické kriminality, které vznikají pod Krajskými ředitelstvími policie. Útvary využívají především policejní systém AMOS, případně CDO, což je datový sklad integrující data z informačních systémů ETŘ, LOOK a D-Zbraně. Systém AMOS slouží k procházení platné metodiky, především k zjišťování společných atributů pachatelů trestné činnosti, tyto atributy vkládají zpracovatelé spisů. Provedenou analýzou v systémech AMOS nebo CDO je možné propojit zpracovatele spisů, kteří mají ve spisech společné atributy u osoby pachatele.

Analýzami trestních spisů ze strany Služby kriminální policie a vyšetřování a vyšších organizačních článků policie dochází k zjišťování dalších informací k jednotlivým skutkům a taktéž k operativnímu předávání informací mezi zpracovateli trestních spisů. Samozřejmě pak může docházet ke slučování trestních spisů, což je pro ekonomičnost a hospodárnost trestního řízení nezbytné a více než žádoucí. opačném případě pak dochází k několika totožným žádostem ke stejným bankovním účtům, dochází ke zbytečnému opakovanému podávání žádostí ze strany několika různých zpracovatelů, dublujícím se žádostem o výslech majitelů bankovních účtů, přičemž mnozí již k věci vypovídali a podobně. Toto samozřejmě představuje administrativní průtahy v celém vyšetřování věci a snižuje případnou možnost objasnění.

Další problém prověřování a vyšetřování v problematice kybernetické kriminality představuje absence specialistů a expertů daného oboru, kteří jsou ve služebním poměru příslušníků bezpečnostního sboru, což se pojí s absencí řádného a odpovídajícího finančního ohodnocení těchto expertů a specialistů ze strany státu a bezpečnostního sboru jako takového. Většina specialistů a expertů pracuje jako externí a civilní pracovníci, nebo s Policií České republiky spolupracují na základě dobré vůle. Experti a specialisté, kteří nikdy nemohou mít takové finanční ohodnocení, jaké by dostali v soukromém sektoru se nebudou do práce po Policii České republiky hrnout, ba naopak, pokud policista disponuje znalostí v oblastech kybernetické bezpečnosti, znalostí výpočetní techniky, softwarem a hardwarem těchto zařízení, ve většině případů dostane v řádu několika měsíců či let lukrativní nabídku z civilního sektoru, které se práce a zejména finanční ohodnocení

ve státní správě nemůže rovnat. Proto dochází k odlivu expertů a specialistů, taktéž s přihlédnutím k tomu, že většina těchto policistů již má nárok na výsluhový příspěvek a nachází se ve vyšších tarifních třídách. Tento trend se sbor pokouší korigovat tím, že právě školí mladé policisty a zájemce o danou problematiku. Jaký bude konkrétní výsledek těchto snah, ukáže s odstupem několika let čas. Je zřejmé, že osvojení si problematiky výpočetní techniky, včetně prověřování a vyšetřování kybernetické kriminality, není otázkou dní, ani měsíců, ale spíše let. Proto pro dobré fungování bezpečnostního sboru v tomto odvětví je třeba metodicky vést a dále více vzdělávat policisty, jelikož současný trend vzdělávání v řádu několika jednotek školení ročně, není plně postačující, a to ani pokud jde o kapacitu těchto školení.

Je zřejmé, že prověřování a vyšetřování kybernetické kriminality probíhá za využití výpočetní techniky, už tento základní aspekt je velmi problematický a nákladný, každý kvalitní hardware, software, nebo přímo uživatelsky přívětivá aplikace pomáhající k vyšetřování je pro bezpečnostní sbor velmi drahou záležitostí, a pokud se již nějaký takový software zakoupí, tak se jedná jen o několik jednotek licencí, kdy software využívají pouze specializované útvary Policie České republiky, a to většinou s celostátní působností (NCOZ, NCTEKK a podobně). Je zřejmé, že výpočetní technika na základních útvarech a taktéž na nižších útvarech Služby kriminální policie a vyšetřování naprosto nedostačuje k prověřování uvedené kriminality. Jedná se o kancelářské stroje, které mají jen základní nastavení, velmi malé výpočetní parametry, nejsou řádně připojeny z důvodu bezpečnosti k internetovému prostředí, ale pouze do sítě intranet, v případě připojení do internetové sítě se musí přistupovat k takové síti prostřednictvím vzdáleného přístupu z počítače pomocí aplikací, jež samozřejmě zpomalují provoz, a veškeré informace se musí duplikovat přes vzdálený server do počítače zpracovatele. Z výše uvedených důvodu většina zpracovatelů spisů týkajících se IT kriminality, včetně autora této práce, do internetového prostředí během prověřování předmětného typu kriminality přistupuje ze svých vlastních soukromých výpočetních zařízení, notebooků, mobilních telefonů apod. Zpracovatelé jsou v zájmu nezbytně účinného prověření celé věci k získání všech potřebných dat a informací nuceni užívat svých

vlastní redukce, paměťové karty, flashdisky, včetně svých osobních externích harddisků, externích vypalovacích mechanik a vlastních externích blue-ray mechanik. Je zřejmé, že instituce Policie České republiky doposud není uspokojivě finančně připravena ani vybavena k optimálnímu chodu při šetření v oblasti na kybernetické kriminality, zásadní roli zde v této problematice sehrává bohužel rozpočtové podhodnocení technického zázemí podpory a vybavenosti. Bezpochyby není dále udržitelné, aby zpracovatel zabývající se IT kriminalitou, v současné době nedisponoval základními prvky výpočetní techniky nebo aby s ní disponoval toliko jeden pracovník za celý územní odbor.

I kdyby bezprostředně uvedené problémy, týkající se jak navýšení finančních prostředků pro technické zázemí, tak vzdělávání policistů a zájemců o prověřování a vyšetřování kybernetické kriminality, byly vyřešeny, je třeba vzít v potaz další neméně důležitou skutečnost. Z osobní zkušenosti autora této práce získané dlouhodobějším monitoringem a diskusí s dalšími příslušníky Policie České republiky totiž vyplývá zjištění, že práce v odvětví kybernetické kriminality pro značnou část policistů není nikterak zajímavá. Velké množství policistů na základních organizačních článcích a na nižších útvarech Služby kriminální policie a vyšetřování nemá k výpočetní technice téměř žádný vztah, případně jen velmi obecný, a to z pohledu pouhého uživatele příslušné výpočetní techniky. Mnohdy se stává, že na popsaných útvarech Policie České republiky činí policistům problém i základní ovládání počítače a jeho základních součástí operačního systému. Uvedené potíže prostupují napříč celým policejním sborem. Často bývá především pro déle sloužící policisty (existují samozřejmě i čestné výjimky) velmi složité učit se novým postupům a technologiím. Setkáváme se s takovými názory, že postačuje znát pouze základní ovládání počítače. Osvojování si nových vědomostí v oblasti výpočetní techniky a jejich následná aplikace v praxi je pro ně složitější a obtížnější. S ohledem na poznatky vývojové psychologie je samozřejmě přirozené (právě s ohledem na jejich přibývající věk), že jim proces učení a zvládnutí jednotlivých poznatků mnohdy trvá déle než jejich mladším kolegům, u některých z nich lze bohužel zaznamenat i zjevné obavy, psychický blok či dokonce nechuť k získávání jednotlivých poznatků a praktických postupů, jež se v však v jejich další

policejní práci jeví jako nezbytné a nutné. Kybernetická kriminalita, jejíž nárůst je za posledních několik let bezpochybně enormní, představuje pro déle sloužící policisty zcela novou záležitost. Záležitost, kde se takřka v žádném bodě nemohou opřít o svou dosavadní získanou praxi, a možná právě proto v nich vyvolává zřejmý odpor. Odpor v tomto případě lze chápat jako strach z neznáma. Tento problém zřejmě značnou měrou může vyřešit generační obměna policistů, k níž postupem času již nyní dochází. Dnešní mladí lidé, mládež i děti mají od raného věku k internetovému prostředí, aplikacím a dalším zařízením mnohem blíže a chovají k tomuto všemu velmi (někdy až přespříliš) pozitivní vztah. Právě uvedená slova ovšem nikterak neznamenají, že by se déle sloužící policisté neměli v celé problematice kybernetické kriminality vzdělávat, být v ní průběžně vzděláváni bezpečnostním sborem a sami se v ní zdokonalovat. Pokud však hodlají v předmětném odvětví stačit svým mladším kolegům, je třeba na sobě dále intenzivně pracovat, obrazně řečeno „neusnout na vavřínech“ ve smyslu dosavadních výsledků a odsloužených let.

Závěr

V samotném závěru této práce je nutné zdůraznit, jak je ostatně nastíněno již v jejím úvodu, že otázka kriminality podvodných útoků v informačních a komunikačních technologiích je velmi problematickou záležitostí, a to jak pro veřejnost, tak pro policisty, vyšetřovatele a další specialisty, kteří se tímto druhem kriminality zabývají. Nejdůležitější část při prověřování těchto útoků orgány činnými v trestním řízení tkví především v prvotních neodkladných a neopakovatelných úkonech, ostatně jako u ostatních dalších typů kriminality. Zde ovšem specificky policejní orgán, který věc prvotně eviduje, musí spolehnout na svou vlastní zkušenost a na získané a v praxi osvojené poznatky z této problematiky. Stěžejními body v boji s kriminalitou podvodných útoků v informačních a komunikačních technologiích jsou především tyto: řádné vyškolení a metodické vedení, dále pak možnost disponovat kvalitní výpočetní technikou, což (jak je v této práci ostatně uvedeno) v současné době představuje jeden z největších problémů u Policie České republiky, ačkoliv v poslední době se na uvedený nedostatek pokouší jmenovaný bezpečnostní sbor postupně zaměřit své síly a prostředky.

Ve věci podvodných útoků s využitím sociálního inženýrství jde především o to uvědomit si nebezpečnost jednání útočníka při postupné a narůstající manipulaci s obětí, úskalí snadno získané důvěry oběti, která v mnoha případech stále důvěřuje útočníkovi, své finanční prostředky zasílá na základě útočníkových výzev opakovaně a takřka slepě věří, že své peníze dostanou zpět v ideálním případě několikanásobně zúročené (princip utopených peněz). Ostatně kdyby útočník osvědčenými psychologickými taktikami v oběti nevzbudil absolutní (často až bezmeznou) důvěru, žádné finanční prostředky by mu oběť nezaslala. Oběti výše popisovaných útoků často podléhají mylnému zdání, že celou věc mají pod svou kontrolou a útočník jim svými pokyny pouze vytváří jakousi asistenci či technickou podporu. U osob, jež se v on-line prostředí hůře orientují nebo se neorientují vůbec a neznají problematiku těchto podvodů nastává tato situace daleko častěji. K tomu se váže samozřejmě možnost využití nejrůznějších preventivních opatření, a to zejména osvěta zaměřená právě na potencionální oběti. Ta v současné době již probíhá, mimo jiné i za součinnosti bankovních

institucí (například reklamní kampaň klikač a volač – ČSOB), nebo dokonce i majitelů aplikací pro vzdálený přístup do zařízení (aplikace AnyDesk a další).
Jak je v práci v předchozích odstavcích uvedeno, pro prověřování protiprávního jednání páchaného v kyberprostoru jsou pro orgány činné v trestním řízení důležité prvotní informace, jež lze získat především od poškozeného. Ten by v ideálním případě měl plně spolupracovat s policejním orgánem (souhlas s prolomením bankovního tajemství, souhlas s prolomením údajů o telekomunikačním provozu, ohledání aplikací, zajištění komunikací a podobně), zároveň pak policista, který věc eviduje, musí být s danou problematikou dobře seznámen a v ní vyškolen. Při prvotním výslechu obětí je tedy velmi důležité zaměřit se na jednotlivé atributy (poznávací znamení, údaje) vztahující se k osobě pachatele. Osobní údaje pachatelů bývají ve většině případů smyšlené, časté bývá též zneužití osobních údajů reálných pracovníků bank, příslušníků Policie ČR, všeobecně uznávaných autorit a podobně. Tento atribut pro prověřování věci je dále využíván jako takzvaný doplňkový atribut, lze k němu v jistých případech přihlédnout například při slučování trestních spisů a vedení společných řízení ve věci, ačkoliv sám o sobě pouze jen doplňkový atribut pro slučování trestních spisů nepostačuje. Jelikož se jedná o velmi propracovanou trestnou činnost, která jeví známky organizované trestné činnosti, je důležité zaměřit se především na zajišťování peněžních prostředků, které útočníci vylákali z obětí, a tím jim zamezit přístup k dalším finančním příjmům, jež pachatelé potřebují především pro své další páchání (nákup GMS modulů, nových sim karet, výpočetních zařízení, jakými jsou počítače, mobilní telefony a podobně). Velmi důležitým atributem pro prověřování těchto podvodů jsou čísla bankovních účtů, čísla kryptopeněženek nebo další údaje vztahující se ke konkrétním platebním transakcím vyžádané u bankovních i nebankovních institucí zajišťující převody finančních prostředků). Právě tyto údaje a informace mohou vést k identifikaci a následnému vypátrání útočníků, dalších obětí, případně prostředníků („bílých koní“), kteří mohou k objasnění přispět svou výpovědí, často i cestou mezinárodní spolupráce. Zde se opět naskýtá možnost rozkrýt a vysledovat jednotlivé posloupnosti v toku finančních prostředků, za jehož pomoci útočníci získávají finanční prostředky do své moci, ať už jde o výběry z bankomatů či další rozličné způsoby převodu peněz umožňující ve finále výplatu v hotovosti

a následnou legalizaci výnosů z trestné činnosti. Pokud se podaří pachatele uvedené trestné činnosti vypátrat, přičemž reálná šance v situaci zde popsané skutečně existuje, musí policejní orgán opět neprodleně reagovat a okamžitě se výše popsaným způsobem neodkladného úkonu v souladu s ustanovením § 79a odst. 1 trestního řádu pokusit finanční prostředky zajistit, vrátit je majiteli, případně dále a detailně sledovat tok finančních prostředků. Webová stránka, resp. doména stránek na nichž útočníci lákají oběti, představuje základní neměnný a hlavní atribut, díky němuž lze pachatele (alespoň na určitou dobu, než vytvoří doménu jinou) identifikovat, případně i paralyzovat, tedy pokusit se přes distributora domény předmětnou webovou stránku zablokovat (například cz.nic správce webových domén .cz). Zároveň se jedná o atribut, na jehož základě je v současné době umožněno slučování trestních spisů. Na základě uvedených domén vznikají na Policejním prezidiu jednotlivé metodiky pro slučování a společná řízení při prověřování těchto skutků. Společné řízení v těchto případech je z důvodu ekonomičnosti, hospodárnosti a celkové praktičnosti trestního řízení velmi žádoucí. Hlavní zpracovatel totiž těchto spisů nemusí provádět desítky, či stovky žádostí na jednotlivé instituce zvlášť, ale naopak postačuje zaslat jednu žádost, na spisech se podílejí týmy zpracovatelů, kteří zodpovídají za svou práci a dobře se v ní orientují. Zároveň vyšší organizační články disponují lepší výpočetní technikou, softwarem i znalostmi dané problematiky. Páchání útoků není ohraničené žádným místem, nebo hranicemi, proto se jistá neochota ke slučování trestních spisů v určitých případech jeví jako jeden z největších problémů při vyšetřování této trestné činnosti. V každém jednotlivém spise zvlášť mohou být jen části, jakési střípky informací vedoucích k možné identifikaci útočníka, pokud se tyto střípky nepodaří spojit v jeden celek, k odhalení pachatele nedojde, a ten nadále spravedlnosti uniká. Právě k vyřešení této problematiky vznikají postupně útvary analytiky a kybernetické kriminality.

Email, telefonní číslo, IP adresa, včetně údajů zjištěných z komunikačních aplikací a aplikací pro vzdálený přístup do zařízení představují další důležité atributy pro možné rozpoznání pachatele. Samozřejmě, že technicky zdatným a moderně vybaveným útočníkům nečiní problém skutečný kontakt zastřít či jakkoliv pozměnit,

v případě telefonního čísla útočníka se navíc často jedná o předplacenou službu, tedy bez uvedení jména a příjmení jeho majitele, takováto sim-karta je užita pouze pro páchání trestné činnosti a dále z telefonu většinou odstraněna. Samostatnou kapitolou pak zůstávají v této práci detailněji popsaná anonymizovaná (spoofovaná) telefonní čísla či emailové adresy. Častá je i situace, kdy pachatel neanonymizuje emailovou adresu, ale svou IP adresu, tedy IP adresu, z níž na email přistupuje a emailové schránky zakládá taktéž jen pro páchání trestné činnosti. V současné době je taktéž hojně využívána nepříznivá politická situace zemí, které jsou v určitém válečném konfliktu, pachatelé svou trestnou činnost páchají právě z těchto zemí, a pro policejní orgán je tak vlastně nemožné se těchto pachatelů, jakkoliv dále dopátrat. Případně informace zjištěné během šetření ve věci vedou například (a velmi často) do Ruské federace nebo na okupované území Ukrajiny, což opět činí prověřování a vyšetřování těchto skutků velmi problematickou, prakticky neřešitelnou záležitostí. Většina útočníků totiž nepochází z České republiky ani zde většinou nežije. Je tedy zřejmé, že objasněnost této kriminality meziročně klesá a je velmi nízká oproti jiné kriminalitě.

Výskyt kriminality podvodných útoků v informačních a komunikačních technologiích bude dle všeho (i podle názoru autora této práce) dále narůstat, taktika útočníků bude stále propracovanější a složitější na objasnění, oprávněnou hrozbu tvoří bezesporu technologický progres umělé inteligence a dalších softwarových aplikací. Zároveň je ale velmi důležité kriminalitu v IT technologiích stále detailněji dokumentovat, protože stejně jako v minulosti nebylo téměř možné trasovat kryptoměny (viz Bitcoin) a v současné době toto možné je, je více než pravděpodobné, že dojde taktéž k posunu ve vytvoření nových účinných nástrojů pro potřeby policejních orgánů, jež zpětně objasní správně zaevidovanou trestnou činnost, která je páchána v současnosti. Stejně jako se neustále zdokonalují útočníci, časem i policejní orgány dojdou dále v prověřování a vyšetřování. Je třeba se zaměřit na rozšíření platné legislativy ve vztahu k on-line prostředí, reklamám umisťovaných na sociálních sítích, ve webových prohlížečích, v neposlední řadě pak na zvýšení financování rozpočtu bezpečnostního sboru jednak z důvodu řádného ohodnocení expertů a specialistů v oboru IT, jednak

ve věci zakoupení kvalitní výpočetní techniky, pomocí níž by prověřování a vyšetřování kybernetické kriminality bylo efektivnější, a především daleko rychlejší

Seznam použité literatury

Monografie

DONÁT, Josef, TOMÍŠEK Jan, PRÁVO V SÍTI, průvodce právem na internetu, Praha: C. H. Beck, 2016, ISBN 978-80-7400-610-4. [citováno 2024-02-09]

KOLOUCH, Jan. CyberCrime. Online. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf. [citováno 2024-02-09].

STROUKAL, Dominik a SKALICKÝ, Jan. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. Třetí rozšířené vydání. Finance pro každého. Praha: Grada Publishing, 2021. ISBN 978-80-271-1043-8. str. 28-29. [citováno 2024-02-09].

KOLOUCH, J. a BAŠTA, P. CyberSecurity. 1. vydání. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-8. [citováno 2024-02-09].

Zákonná úprava

Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád) v posledním znění

Zákon č. 273/2008 Sb., o Policii České republiky v posledním znění.

Webové stránky a internetové zdroje

KINTR, Lukáš. Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022. Online. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Dostupné z: https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/. [citováno 2024-02-09].

VINČÁLEK, Jakub a MORAVČÍK. Ondřej. Policie České republiky: Vývoj registrované kriminality v roce 2023. Online. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2023.aspx. [citováno 2024-02-09].

BURÝŠEK, Jiří. YOUTUBE – KANÁL JIRKA VYSVĚTLUJE VĚCI. Poslal jsem podvodníkovi 300 000 Kč. Online. Dostupné také z: https://www.youtube.com/watch?v=bre2eJsAdhM. [citováno 2024-02-09].

BLAHNÍKOVÁ, Irena. VLTAVA LABE MEDIA. Boleslavský deník. Online. Dostupné také z: https://boleslavsky.denik.cz/zlociny-a-soudy/boleslavsko-podvod-kdyptomena-investice-policie-cr-20062023.html. [citováno 2024-02-09].

BLAHNÍKOVÁ, Irena. VLTAVA LABE MEDIA. Boleslavský deník. Online. Dostupné také z: https://boleslavsky.denik.cz/zlociny-a-soudy/mlada-boleslav-policie-cr-

podvodnici-prehled-pripady-rok-2023-05012024.html?cast=3. [citováno 2024-02-09].

CHAROUSKOVÁ, Šárka. STATUTÁRNÍ MĚSTO MLADÁ BOLESLAV. Mb-net. Online. Dostupné také z: https://mb-net.cz/internetovi-podvodnici-pripravili-muze-z-boleslavi-o-pul-milionu-korun/d-78260/p1=63082. [citováno 2024-02-09].

HRABĚ, Jan. INCORP A. S. Ukrajina předala české policii pětici osob, má jít o podvodníky. Online. Dostupné také z: https://eurozpravy.cz/domaci/ukrajina-predala-ceske-policii-petici-osob-ma-jit-o-podvodniky.e3vk52tb. [citováno 2024-02-09].

MBANK S.A. Krádeže osobních údajů. Online. Dostupné také z: https://www.mbank.cz/blog/post,735,kradeze-osobnich-udaju.html. [citováno 2024-02-09].

KŘÍŽEK, Martin. IROZHLAS. Únik dat klientů Komerční banky je opravdu vážné pochybení, říká právník z Iuridicum Remedium. Online. Dostupné také z: https://www.irozhlas.cz/zpravy-domov/unik-dat-klientu-komercni-banky-je-opravdu-vazne-pochybeni-rika-pravnik-z-iuridicum-remedium_201307231846_vkourimsky. [citováno 2024-02-09].

JANČOVÁ, Andrea. A11 S.R.O. Další podvod na klienty bank! Tentokrát se ozývá fiktivní ruský bankéř. Online. Dostupné také z: h https://nasregion.cz/dalsi-podvod-na-klienty-bank-tentokrat-se-ozyva-fiktivni-rusky-banker-255244/. [citováno 2024-02-09].

NEUBAUEROVÁ, Tereza. POLICIE ČESKÉ REPUBLIKY – TÝDENÍK POLICIE. Rusky mluvící falešný bankéř se zaměřuje na Ukrajince a Rusy žijící v České republice. Online. Dostupné také z: https://tydenikpolicie.cz/rusky-mluvici-falesny-banker-se-zameruje-na-ukrajince-a-rusy-zijici-v-ceske-republice/. [citováno 2024-02-09].

MOJŽÍŠ, Jiří. POLICIE ČESKÉ REPUBLIKY. Usnesení podle § 79a odst. 1 trestního řádu. Online. Dostupné také z: https://www.policie.cz/soubor/usneseni-o-zajisteni-veci-79a-odst-1-tr-r-ceska-sporitelna-a-s-pdf.aspx. [citováno 2024-02-09].

VOŘÍŠEK, Lukáš. INSMART. Co je to spoofing? Online. Dostupné také z: https://insmart.cz/co-je-spoofing/. [citováno 2024-02-09].

KROFTOVÁ, Hana. NEBUĎ BIT – BUĎ IN - BITCOINMATY. Online. Dostupné z: https://www.policie.cz/clanek/nebud-bit-bud-in-bitcoinmaty.aspx. [citováno 2024-02-09].

ČESKOSLOVENSKÁ OBCHODNÍ BANKA. Braňte se rozumem. Online. Dostupné z: https://www.csob.cz/branteserozumem. [citováno 2024-02-09].

FINANČNÍ ANALYTICKÝ ÚŘAD. Analytická činnost. Online. Dostupné z: https://fau.gov.cz/analyticka-cinnost#analyticka-cinnost. [citováno 2024-02-09].

Digitální stopa. IT Slovník. Online. Dostupné z: https://it-slovnik.cz/pojem/digitalni-stopa. [citováno 2024-02-09].

Romance Scam. Policie České republiky. Online. Dostupné z: https://www.policie.cz/soubor/romance-scams.aspx. [citováno 2024-02-09].

Facebook Messenger. META. Facebook.com. Online]. Dostupné z: https://www.messenger.com/features?locale=cs_CZ. [citováno 2024-02-09].

WhatsApp, WHATSAPP IRELAND LIMITED. Whatsapp.com. Online. Dostupné z: https://www.whatsapp.com/?lang=cs_CZ. [citováno 2024-02-09].

Telegram. Telegram.org. Online. Dostupné z: https://telegram.org/. [citováno 2024-02-09].

Viber. VIBER MEDIA. Viber. Online. Dostupné také z: https://www.viber.com/en/. [citováno 2024-02-09].

AnyDesk. ANYDESK. Anydesk.com. Online. Dostupné z: https://anydesk.com/en. [citováno 2024-02-09].

TeamViewer.TEAMVIEWER. TeamViewer. Online. Dostupné také z: https://www.teamviewer.com/cs/. [citováno 2024-02-09].

SupRemo. NANOSYSTEMS. SupRemo. Online. Dostupné také z: https://www.supremocontrol.com/. [citováno 2024-02-09].

Bitcoin. BITCOIN. Bitcoin. Online. Dostupné také z: https://bitcoin.org/en/. [citováno 2024-02-09].

Binance. BINANCE. Binance. Online. Dostupné také z: https://www.binance.com/cs. [citováno 2024-02-09].

Coinbase. COINBASE. Coinbase. Online. Dostupné také z: https://www.coinbase.com/. [citováno 2024-02-09].

Kraken. PAYWARD, INC. Kraken. Online. Dostupné také z: https://www.kraken.com/. [citováno 2024-02-09].

Bitstamp. BITSTAMP USA, INC. Bitstamp. Online. Dostupné také z: https://www.bitstamp.net/. [citováno 2024-02-09].

Blockchain. BLOCKCHAIN.COM. Blockchain.com. Online. Dostupné také z: https://www.blockchain.com/. [citováno 2024-02-09].

WalletExplorer. CHAINALYSIS. Walletexplorer.com. Online. Dostupné také z: https://www.walletexplorer.com/. [citováno 2024-02-09].

Blockchair. BLOCKCHAIR. Blockchair. Online. Dostupné také z: https://blockchair.com/. [citováno 2024-02-09].

Elliptic. ELLIPTIC. Forensis. Online. Dostupné také z: https://www.elliptic.co/. [citováno 2024-02-09].

Reactor. CHAINALYSIS. Reactor. Online. Dostupné také z: https://www.chainalysis.com/. [citováno 2024-02-09].

IP adresa. Mojeip.cz. Online. Dostupné z: https://www.mojeip.cz/. [citováno 2024-02-09].

KYBERTEST.CZ. Buďte na internetu v bezpečí. Kybertest.cz. Online. Dostupné z: https://www.kybertest.cz. [citováno 2024-02-09].

MINISTERSTVO VNITRA. Prevence kriminality. Online. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/. [citováno 2024-02-09].

MINISTERSTVO VNITRA. Kyberkriminalita. Online. Dostupné z: https://prevence-kriminality.cz/prevence-kriminality/kyberkriminalita/.
[citováno 2024-02-09].

ANYDESK. How to Avoid Remote Access Scams. Online. Dostupné z: https://anydesk.com/en/abuse-prevention. [citováno 2024-02-09].