POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní
Katedra kriminální policie

ZVLÁŠTNOSTI METOD PROVĚŘOVÁNÍ A VYŠETŘOVÁNÍ KYBERNETICKÉ KRIMINALITY

DIPLOMOVÁ PRÁCE

SPECIFICITIES OF THE CYBER CRIME SCREENING AND INVESTIGATION METHODS

DIPLOMA THESIS

Vedoucí práce:
Ing. Bc. Luděk Michálek, Ph.D.

Autor práce:
Bc. Václav Pech

2024

Čestné prohlášení:

Prohlašuji, že jsem diplomovou práci na téma „**Zvláštnosti metod prověřování a vyšetřování kybernetické kriminality**“ zpracoval samostatně, je mým původním autorským dílem. Veškerou literaturu, prameny a zdroje informací, z nichž jsem čerpal a byly použity k sepsání této práce, řádně v práci cituji v poznámkách pod čarou a jsou uvedeny v seznamu použitých pramenů a literatury.

Bolechovice 2024 dne .. ..

Václav Pech

Poděkování:

Chtěl bych poděkovat panu doktorovi Ing. Bc. Luďkovi Michálkovi, Ph.D. za to, že mi umožnil zpracování této diplomové práce a také za jeho aktivní a vstřícný přístup.

Anotace

Diplomová práce na téma „ZVLÁŠTNOSTI METOD PROVĚŘOVÁNÍ A VYŠETŘOVÁNÍ KYBERNETICKÉ KRIMINALITY“ se zabývá současnými možnostmi prověřování kybernetické kriminality, zejména z pohledu policejních orgánů. Práce je rozdělena na 2 části, teoretickou a praktickou. V teoretické části je obsaženo vymezení a vysvětlení základních pojmů z oblasti informačních technologií a pojmů spojených s kybernetickou kriminalitou, v části praktické jsou popsány úkony spojené s problematikou prověřování a vyšetřování kybernetické kriminality, na nichž záleží mimo jiné efektivita a objasněnost tohoto typu kriminality. V praktické části je obsažen rozbor aktuálních případů z oblasti kybernetické kriminality, který podrobněji ukazuje problematiku prověřování kybernetické kriminality. K práci je zpracována stručná příručka pro policisty.

Klíčová slova

Kybernetická kriminalita, finanční prostředky, neznámý pachatel, poškozený, internetové stránky, důkazní prostředky, digitální stopa.

Annotation

The diploma thesis on the topic "SPECIFICITIES OF THE CYBER CRIME SCREENING AND INVESTIGATION METHODS " deals with the current possibilities of investigating cyber crime, especially from the point of view of police authorities. The work is divided into 2 parts, theoretical and practical. The theoretical part contains the definition and explanation of basic concepts from the field of information technology and concepts associated with cybercrime, the practical part describes actions connected with the issue of screening and investigating cybercrime, which depends, among other things, on the effectiveness and clarity of this type of criminal activity. The practical part contains an analysis of current cases in the field of cybercrime, which shows the issue of cybercrime screening in more detail. A brief manual for police officers is prepared for the work.

Keywords

Cybercrime, funds, unknown perpetrator, victim, website, evidence, digital trail.

Použité zkratky:

TZ – Zákon trestní zákoník, zákon č. 40/2009 Sb.
TŘ – Zákon o trestním řízení soudním (trestní řád), zákon č. 141/1961 Sb.
ZPPP – závazný pokyn policejního prezidenta
Kyber. Kriminalita – Kybernetická kriminalita
Bank. Účet – Bankovní účet
PČR – Policie České republiky
OOP – Obvodní oddělení policie
SKPV – Služba kriminální policie a vyšetřování
OKTE – Odbor kriminalistické techniky a expertíz
KÚ – Kriminalistický ústav
IS – Informační systém
PC – Počítač
EU – Evropská Unie
IT – informační technologie

Obsah

1 ÚVOD

Lidstvo se za dobu své existence naučilo využívat spoustu přírodních sil a prostředků ve svůj prospěch. Bohužel mnohdy objevy nesloužily a neslouží k posunu lidstva jako celku směrem do budoucnosti, ale byly a jsou použity jako prostředky a pomůcky pro jednotlivce či skupiny osob za účelem profitu či získání jiných výhod. K obdobnému případu došlo i v případě rozvoje informačních a komunikačních technologií. Tento rozvoj umožnil posun lidstva směrem do budoucnosti, ale zároveň umožnil i rozvoj protiprávních činností využívajících technologie, znalosti a možnosti, které vyplývají z tohoto rozvoje, což se projevuje v celkové kriminalitě, kdy postupně vzniklo odvětví kriminality, jenž se souhrnně nazývá kybernetickou kriminalitou. S ohledem na vývoj dané problematiky, zejména s ohledem na enormní nárůst v posledních letech, je více než jisté, že tato kriminalita bude zastávat stále větší procento výskytu v celkovém množství kriminality. Z toho vyplývá, že se s touto problematikou setkává a bude setkávat stále větší množství osob, jenž se zabývají nejen prověřováním a vyšetřováním kriminality, ale zároveň i občanů jakožto obětí, poškozených, svědků nebo i pachatelů této trestné činnosti.

Vytvoření této diplomové práce je motivováno skutečností, že prověřování a vyšetřování kybernetické kriminality je v některých případech zatíženo chybami a nedostatky, které mají ve svém důsledku důležitý význam pro řádné objasnění této kriminality a stíhání pachatelů. Tyto nedostatky pramení z různých okolností a skutečností, proto si tato diplomová práce klade za úkol popsat problematiku kybernetické kriminality, vymezit její základní pojmy, určit základní metodiku vyšetřování kybernetické kriminality a zdůraznit její specifika. Z tohoto plyne vymezení typického způsobu páchání této kriminality, typické počáteční úkony, kriminalistické stopy, zvláštnosti výslechu a dalších úkonů. V rámci získávání informací pro prověřování budou nastíněny možnosti získávání informací z otevřených (volně dostupných) i policejních zdrojů. Na aktuálních reálných případech z oblasti kybernetické kriminality bude popsán stručný průběh prověřování a následně bude proveden jejich

rozbor, v němž v jednotlivých případech bude po popsání konkrétního případu provedeno zhodnocení daného případu s nastíněním prakticko-teoretického postupu týkajícího se chyb, nedostatků, ale i správně provedených úkonů. V popisu případu bude také uvedeno, zda se případ podařilo objasnit a zahájit stíhání konkrétní osoby pachatele či nikoliv.

Koncovým výstupem této diplomové práce bude vytvoření jednoduché příručky pro zkvalitnění zejména prvotního zpracování případů kybernetické kriminality.

Metody použité k vypracování této diplomové práce jsou použité dle cíle jednotlivých částí diplomové práce, v teoretické části a částečně i v praktické části je použit popis vysvětlujícího charakteru, v části zobecňující některé aspekty kybernetické kriminality je použita metoda logické indukce a u rozboru jednotlivých případů z praxe je využita metoda analýzy.

2 TEORETICKÁ ČÁST

2.1 Vymezení pojmů

Kybernetická kriminalita je specifická kriminalita, která je páchána za užití moderních technologií, prostředků a postupů zpracování a transferu dat. Proto je pro její prověřování a vyšetřování nutné se alespoň částečně orientovat v těchto technologiích, bez znalostí by nebylo možné důsledně vést prověřování, vyšetřování a vyhodnocovat relevantní váhu jednotlivých informací, jež by mohli sloužit jako důkazní prostředky. Podstatná je samozřejmé také skutečnost, že technologie i postupy se neustále vyvíjí a pachatelé stále přicházejí s novými způsoby páchání této kriminality. Z toho plyne náročnost pro zpracovatele kybernetické kriminality tkvící v tom, aby se nedostal do stavu stagnace, ale naopak své znalosti a schopnosti rozvíjel.

Pro základní orientaci v problematice kybernetické kriminality jsou v této diplomové práci uvedeny základní pojmy, které jsou rozděleny do dvou kategorií:

- pojmy související s informačními technologiemi,
- pojmy související s prověřováním a vyšetřováním kybernetické kriminality.

U kybernetické kriminality je nutné zmínit další specifikum, a to jest skutečnost, že zpracovatel této problematiky mnohdy za účelem zefektivnění postupu a získání informací spolupracuje s dalšími orgány státní správy či specifickými organizačními články bezpečnostních sborů. Z tohoto důvodu je v teoretické části této diplomové práce zařazena podkapitola, jenž se věnuje stručnému popisu těchto orgánů a institucí.

2.1.1 Pojmy související s informačními technologiemi

Kybernetický prostor – je digitální prostředí umožňující vznik, zpracování a výměnu informací, je tvořen informačními systémy, službami a sítěmi elektronických komunikací.[1] Zjednodušeně řečeno je kyberprostor internet jako

[1] Str. 33 učebnice „Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní managment ve vzájemných souvislostech“, kolektiv autorů PAČR, Praha 2020

takový.

Internet – je Globální systém propojených počítačových sítí, které používají standardní internetový protokol (TCP/IP). Internet slouží miliardám uživatelů po celém světě. Je to síť sítí, která se skládá z milionů soukromých, veřejných, akademických, obchodních a vládních sítí, s místním až globálním rozsahem, které jsou propojeny širokou škálu elektronických, bezdrátových a optických síťových technologií.[2]

Intranet – je „Privátní“ (interní) počítačová síť využívající klasické technologie Internetu, která umožňuje zaměstnancům organizace efektivně vzájemně komunikovat a sdílet informace.[3]

Darknet – tímto termínem je označována část internetu, která není dostupná klasickými vyhledávači a je přístupná pouze pomocí speciálního softwaru, jako například Tor. Obsahuje převážně webové stránky, které nejsou veřejně dostupné, ale jsou skryty za anonymizačními službami a šifrováním. Darknet se často spojuje s nelegálními aktivitami, jako je obchodování s drogami, zbraněmi nebo služby hackerů. Označení darkweb je sice podobné, ale je jím myšlena část internetu, která je umístěna na darknetu.

DNS server – je distribuovaný hierarchický jmenný systém používaný v síti Internet. Překládá názvy domén na číselné IP adresy a zpět, obsahuje informace o tom, které zařízení poskytují příslušnou službu (např. přijímají elektronickou poštu či zobrazují obsah webových prezentací) atd.[4]

IP adresa – slouží, jako primární identifikátor každého počítače, který je

---

[2] Str. 59 Výkladový slovník kybernetické bezpečnosti, Petr Jirásek, Luděk Novák, Josef Požár, Policejní akademie ČR v Praze, Praha 2015

[3] Str. 61 Výkladový slovník kybernetické bezpečnosti, Petr Jirásek, Luděk Novák, Josef Požár, Policejní akademie ČR v Praze, Praha 2015

[4] Str. 40 Výkladový slovník kybernetické bezpečnosti, Petr Jirásek, Luděk Novák, Josef Požár, Policejní akademie ČR v Praze, Praha 2015

připojen v počítačové síti. Internetový protokol (z anglického Internet Protocol - zkratka IP) je typem specifického protokolu, díky kterému vůbec servery mohou spolu komunikovat a být vzájemně interoperabilní. Takovému spojení se také pak říká výměna IP adres. IP adresy se přidělují na pokyn příslušné organizace, která má za úkol spravovat, registrovat a vést si evidenci jednotlivých IP adres. Současná světová norma je ohraničena maximem 255. 255. 255. 255 a vyšší hodnoty zatím neexistují. Nejrozšířenější dvě používané verze jsou:

IPv4 – 32 bitové číslo

IPv6 – 128 bitové číslo

Důležitý poznatek je, že jedna adresa se klidně může nacházet i pod více doménových jmen, což se v praxi děje u virtuálních serverů, které běží na jednom jediném fyzickém stroji (v praxi to znamená, že je jedna IP adresa přiřazena více zařízením). Důležitost IP adresy je často terčem negativně manipulujících útoků – tedy spíše se jedná o crackery. Mezi takové zrádné crackerské metody patří např. IP spoofing. Dosti kontroverzním samo o sebe je maskování IP adresy za pomoci anonymního proxy serveru.[5]

Privátní IP adresa – jsou skupiny IP adres definované v RFC 1918 jako vyhrazené pro použití ve vnitřních sítích (např. v rámci firmy). Tyto IP adresy nejsou směrovatelné z internetu. Jedná se o následující rozsahy:

10.0.0.0 – 10.255.255.255,

172.16.0.0 – 172.31.255.255,

192.168.0.0 – 192.168.255.255.[6]

Důležité je to, že pokud jsou zjištěny, jejich lustrací většinou nejsou zjištěny další informace.

Virtuální privátní síť – neboli Virtual private network (VPN) je privátní počítačová síť, která dovolí připojit vzdálené uživatele do cílené LAN (z angličtiny „local area network“ neboli lokální sítě pomocí níž dochází k připojení do sítě) přes

[5] Správa sítě, Správa sítě slovník pojmů. Dostupné z https://www.sprava-site.eu/ip-adresa

[6] Str. 61 Výkladový slovník kybernetické bezpečnosti, Petr Jirásek, Luděk Novák, Josef Požár, Policejní akademie ČR v Praze, Praha 2015

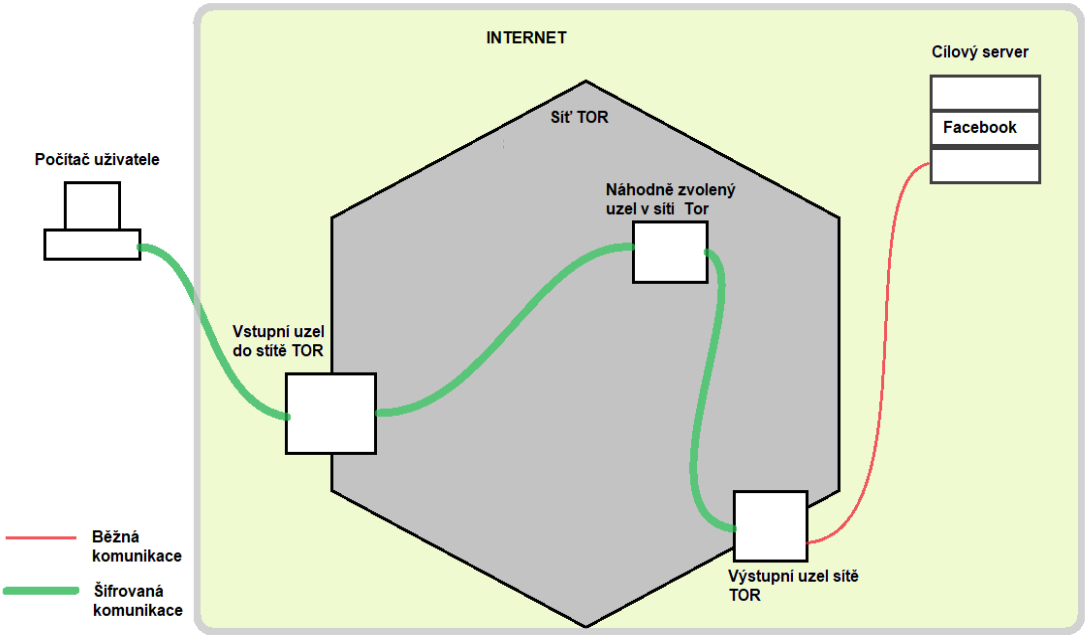
Internet. Bezpečnost se řeší pomocí šifrovaného tunelu mezi dvěma body (nebo jedním a několika). Tím skrývá IP adresu. Při navazování spojení je totožnost obou stran ověřována pomocí digitálních certifikátů.[7] Tímto postupem jsou chráněna data uživatele před případným sledováním.

Síť TOR – je nástupcem Onion routing programu, který byl vynalezen ústavem Amerického námořnictva v polovině 90. let. Síť TOR patří k další generaci. Síť TOR je tvořena tzv. uzly, které z velké části vytváří dobrovolníci. Pro přístup k síti TOR je zapotřebí specializovaní internetový prohlížeč. Veškerá komunikace je několikrát šifrována, včetně IP adresy. Připojení po síti TOR je vždy směřováno přes několik náhodně vybraných uzlů, které se mohou nacházet i na různých kontinentech. Vzhledem k několika vrstvému šifrování je probíhající komunikace skrytá i před správci uzlů. V síti TOR se nachází webové stránky se skrytým umístěním tzv. Onion stránky a další služby. Onion stránky mohou být skryté a hostované v síti TOR. Je možné tyto internetové stránky navštěvovat a užívat bez zjištění serveru, kde se daná Onion stránka nebo služba fakticky nachází. Adresa webové stránky nebo služby v síti tor se skládá z náhodných znaků s koncovkou .onion. Takto vypadá adresa na internetový vyhledavač DuckDuckGo, 3g2upl4pq6kufc4m.onion. Zjištění dat až k cílovému zařízení je prakticky nemožné. Lze zjistit pouze vstupní nebo koncový uzel, nikdy oba najednou. Užití sítě TOR umožňuje procházet internet anonymně, IP adresa uživatele je skryta před webovými stránkami a dalšími internetovými službami. Užitím sítě TOR může pachatel zcela znemožnit zjištění své aktivity na internetu.

Pro přístup do sítě TOR je zapotřebí užívat specializovaný webový prohlížeč, který vylepšuje anonymitu na internetové síti tím, že o zařízení, na kterém je spuštěn, podává k cílové destinaci připojení minimum informací a některé poskytované informace přímo podvrhuje. To značně stěžuje a při správném nastavení prohlížeče zcela znemožňuje identifikaci koncového zařízení na základě poskytnutých informací. TOR prohlížeč má i verzi pro mobilní telefony s operačním systémem Android i iOS. Ochrana ve formě TOR sítě a VPN služby

[7] Str. 217 Výkladový slovník kybernetické bezpečnosti, Petr Jirásek, Luděk Novák, Josef Požár, Policejní akademie ČR v Praze, Praha 2015

se dá kombinovat, tedy lze využít obojí.[8]



Obrázek 1 – znázornění principu fungování sítě TOR

Zjednodušeně řečeno je síť TOR anonymní síť (je to volně dostupný software) pro anonymní komunikaci, jenž popsaným způsobem umožňuje uživateli skrýt svou původní IP adresu.

Pozn. – zajímavé je, že v rámci prověřování kybernetické kriminality bylo nezávisle na sebe od několika bank zjišťováno, jestli je možné se do jejich internetového bankovnictví přihlásit přes TOR. Většina bank se k této možnosti nevyjádřila. Telefonickou konzultací s jejich pracovníky, kteří mají na starosti odpovědi orgánům v trestním řízení, bylo zjištěno, že se touto otázkou příliš nikdo nezabýval. Od většiny dotazovaných bank tedy nebyla získání žádná odpověď. Několik bank však odpovědělo (Česká spořitelna, Komerční banka), kdy po ověření u jejich oddělení IT konstatovali, že to možné je, nedochází ke kontrole ani blokaci těchto přihlášení. Z tohoto vyplývá, že pravděpodobně je tento způsob přihlášení umožněn u všech nebo většiny bank, čímž je v rámci prověřování značně ztíženo

[8] Bakalářská práce Aktuální problémy kriminalistické metodiky vyšetřování podvodů, Oldřich Smetivý, kapitola 4

či téměř znemožněno získání relevantních informací k osobě pachatele v podobě jeho přístupových údajů.

Doména – neboli doménové jméno je unikátní internetová adresa. Její hlavní funkcí je nahrazovat číselný kód v podobě IP adresy, čímž usnadňuje nalezení a navštívení konkrétních webových stránek. Lze si ji představit jako standardní adresu, která se skládá například z názvu ulice a čísla popisného. Pokud by neexistovalo pojmenování ulic, museli by lidé využívat složitých souřadnic k určení pozice budovy. Na stejném principu funguje i doména.

Druhy neboli úrovně domén

Domény se zpravidla dělí do tzv. úrovní. Prakticky popisují jednotlivé části doménového jména jako celku.

Doména I. řádu – v angličtině TLD (top level domain), nachází se na konci za tečkou, jde tedy o koncovku. Rozlišují se 2 druhy, a to geografické (pro Českou republiku „cz“) a generické („com“, „info“ či „org“ a další). Příklad: www.jmenowebu.cz.

Doména II. řádu – jedná se o nejdůležitější typ, protože je to samotný název stránek. Při čtení textu zleva doprava se jedná o část před doménou I. řádu. V současné době v ní lze využít znaky anglické klávesnice. Délka musí být do 63 znaků. Příklad: www.jmenowebu.cz.

Doména III. řádu – lze se setkat i s pojmenováním subdoména. Představuje určité rozšíření domény II. řádu. Příklad: magazin.jmenowebu.cz.[9]

Kryptoměna – je digitální aktivum sloužící jako zprostředkovatel směny využívající silné šifrování za účelem bezpečnosti transakcí. Kryptoměně se říká také cryptocurrency, cryptoměna nebo virtuální měna (například bitcoin nebo etherum). V dnešní době již je mnoho druhů kryptoměn. Její hlavní, a zřejmě nejpřitažlivější vlastností je, že není vydávána centrální bankou, takže je teoreticky imunní proti ovlivňování a manipulaci ze strany vlád. Její hodnota je založena pouze na nabídce a poptávce, což může způsobit silné fluktuace ceny.

[9] Mioweb s.r.o., Mioweb. Dostupné z https://www.mioweb.cz/slovnicek/domena

Kryptoměny také nabízí možnost platby bez přítomnosti třetí strany, nejčastěji banky, transakční náklady jsou u ní minimální. Kryptoměnu je možné koupit nebo těžit ověřováním transakcí, které je však velmi energeticky náročné.[10]

Trading – je rychlé spekulativní prodávání a nakupování finančních instrumentů s cílem profitovat na jejich kursových změnách.[11]

Bitcoinové peněženky – bitcoinová či obecně krypto peněženka je v podstatě ekvivalentem bankovního účtu. Umožňuje přijímat, odesílat a ukládat Bitcoin a další kryptoměny. Rovněž si ji lze představit jako vstupní bod do kryptoměnové sítě. Po jejím vytvoření je k dispozici adresa peněženky a takzvaný privátní klíč.

Typy kryptopeněženek:

- *Webové a mobilní peněženky* – jsou obecně velmi jednoduché a intuitivní, ale při používání webových peněženek existuje několik rizik plynoucích z toho, že provozovatel služby má přístup k privátním klíčům (k heslu od peněženky), čili při používání webových peněženek lze použít u ověřeného provozovatele.

- *Mobilní peněženky* – fungují na obdobném principu webové peněženky, ale dávají možnost ovládat lépe privátní klíč. U mobilních peněženek nastává velký problém ve chvíli, kdy se dostane do telefonu nějaký vir, jako malware nebo spyware, který zaznamenává vše, co na telefonu probíhá.

- *Softwarové peněženky* – lze nainstalovat na počítač či notebook. Jsou relativně bezpečné a jednoduché na ovládání. Potenciální riziko ale nastává v okamžiku, kdy se počítač připojí k internetu nebo pokud je počítač infikovaný virem (malwarem).

-*Hardwarové peněženky* – jsou jednou z nejbezpečnějších možností, jak uchovat a spravovat Bitcoiny a další kryptoměny. Jedná se o fyzické zařízení, které uchovává kryptoměny offline. Peněženka tedy nemůže být napadena hackery, protože není připojena k internetu. Tato zařízení mohou následně být připojena k

[10] CzechWealth spol. s.r.o., CzechWealth, průvodce světem burzy. Dostupné z https://www.czechwealth.cz/slovnik-pojmu/kryptomeny

[11] CzechWealth spol. s.r.o., CzechWealth, průvodce světem burzy. Dostupné z https://www.czechwealth.cz/slovnik-pojmu/trading

počítači, kde lze jednoduše spravovat kryptoměny.[12]

Blockchain – je z angličtiny „blokový řetězec“. V podstatě je to distribuovaná databáze, ve které jsou navždy uloženy veškeré záznamy, které do ní byly vloženy. Pro přirovnání můžeme použít, že je to nekonečná kniha účetních záznamů. Blockchain vlastně není ani tak úplně novou revoluční technologií – všechny prvky, které využívá, tedy internet, kryptografii a přenosový protokol existují již desítky let (kryptografie dokonce mnohem déle). Revoluční na blockchainu tedy nejsou technologie samotné, ale způsob, jakým stávající technologie využívá.

Blockchain umožnil lidem, prostřednictvím internetu vyměňovat nebo vytvářet záznamy zcela bezpečnou cestou, a to bez nějakého prostředníka (například notáře, banky). Na jeho provozu se totiž podílejí místo centrálního správce přímo jeho uživatelé. Každý se může zapojit jak přímo do ověřování transakcí (těžby kryptoměn), tak do hlídání těch, kdo v daném blockchainu transakce ověřuje. Stačí k tomu provozovat takzvaný nod, což není nic jiného než aktuální kopie blockchainové databáze.

Blockchain tedy představuje velmi specifickou formu databáze. Je distribuovaná, nemá centrálního správce, může ji číst kdokoli, ale zapisovat do ní lze jen na základě konsenzu. Ten vzniká prostřednictvím hlasování finančně motivovaných účastníků sítě (tedy alespoň v případě veřejného blockchainu, existují totiž i jiné koncepty). Díky tomu je možné bezpečně a trvale uchovávat data nebo transakce bez nutnosti centrální dohledové autority, a tím pádem také bez jediného snadno zranitelného místa.

O validaci (ověření) se stará samotná síť. Uživatelé, kteří se na validaci transakcí svým hlasováním podílejí, jsou za svoji aktivitu odměňováni v podobě síťových tokenů daného blockchainu (známější jsou zpravidla pod označením kryptoměny, jako je například bitcoin, ethereum, litecoin, apod.). Tyto tokeny snadno směnitelné na specializovaných burzách za státem vydávané peníze. Problém je trochu v tom, že jejich reálná hodnota je velmi obtížně stanovitelná a

[12] ATC computers, ATC Martket. Dostupné z https://www.atcmarket.cz/articles/25470

jejich současná cena je proto do velké míry spekulativní. Blockchain tak vlastně nahrazuje sítě trhy. Mezi jeho důležité stránky z technického hlediska patří stabilita, jednoduchost specifikace a trvalá povaha v čase (je extrémně obtížné jej zfalšovat).[13]

V rámci kryptoměn je blockchain právě to, jak se zaznamenávají transakce. Tedy pomocí něj lze transakce ve světě kryptoměn trasovat.

Počítačový vir – je škodlivý program nebo část programového kódu, který se spustí bez vědomí uživatele. Cílem počítačového viru je zpravidla získání kontroly nad počítačovým systémem nebo jeho částí a následně poškození uživatele samotného (kupříkladu smazáním souborů bez vědomí uživatele).

Ke svému šíření využívá hostitele – jiné soubory, do kterých je vkládán (zkopírováním svého těla) a tyto využívá jako prostředek pro své další přenášení za účelem infikovat další systém. K tomuto šíření využívá zejména spustitelné soubory (EXE, COM, SYS atd.), různé dokumenty (DOC, XLS apod.) nebo samospustitelné přílohy emailové komunikace. V chování počítačového viru lze nalézt paralelu s chováním viru biologického. Je schopen replikovat sám sebe do buněk. Klasický počítačový vir je v dnešní době na ústupu, je vytlačován sofistikovanějšími formami útoku na systém, neboť si s ním dokáže poradit prakticky každý lepší antivirový program.[14]

Počítačový červ (worm) – je druhem počítačového viru. Jedná se o škodlivý kód, jehož cíl je stejný jako u počítačových virů – poškození uživatele, resp. jeho dat. Od počítačového viru se ale liší zejména formou, jakou se šíří. Počítačový červ se dokáže replikovat sám a do dalších počítačových systémů se většinou šíří prostřednictvím počítačových služeb. Takto vytvořené kopie je schopen „na dálku“ aktivovat a spustit. Ke svému šíření rovněž využívají programových chyb systémů a dalších programů, které mají k systému přístup

[13] Alza.cz a.s., Alza.cz. Dostupné z https://www.alza.cz/co-je-blockchain

[14] Projekt Internetem bezpečně, Realizátorem projektu je nezisková organizace you connected, z.s., ISSN 2571-3736. Dostupné z https://www.internetembezpecne.cz/internetem-bezpecne/malware/virus/

nebo mohou ovlivnit běh systému.[15]

Trojský kůň – (Trojan) je škodlivý kód, který je ukryt v počítačovém programu a který se může na první pohled tvářit užitečně. Jde třeba o drobnou hru, spořič obrazovky, anebo právě program na odstranění malwaru. Často využívá legitimitu důvěryhodného zdroje – emailová zpráva s přílohou (v níž je trojský kůň) vytvářející domnění, že pochází např. od společnosti vyvíjející antivirové programy. Název Trojský kůň je odvozen od řecké mytologie, dobytí Troje, protože stejné poslání má trojský kůň v počítačovém světě, protože jeho účelem je často získat moc nad systémem, kam byl v legitimním programu propašován. Jeho cílem je zpravidla: možnost ovládat počítač uživatele útočníkem, manipulace a mazání dat, získávání hesel, ovládání běžících systémů (vzdálené ovládání systému) apod. Na rozdíl od počítačového viru se zpravidla nesnaží o své „samošíření".[16]

Ransomware (ransom je v překladu výkupné) – je jeden z mnoha druhů škodlivého softwaru, kterému se říká malware. Ransomware se vyznačuje tím, že uzamkne plochu uživatelova PC a pro následné odblokování požaduje po uživateli určitou finanční částku, kterou má zaplatit pachateli (nejčastěji cryptopeněženky).

Nebezpečná varianta ransomwaru je ta, která s blokací plochy zároveň šifruje uživatelská data. Ransomware proniká do operačního systému přes vzniklé díry v zastaralém a často neaktualizovaném softwaru jako trojský kůň či worm. Dalším možným způsobem je ten, že uživatelské PC je součástí tzv. armády zombie počítačů (tj., že pachatel kontroluje PC bez vědomí uživatele).[17]

Vzdálený přístup – je postup, který se v IT oblasti používá pro globalizaci

---

[15] Projekt Internetem bezpečně, Realizátorem projektu je nezisková organizace you connected, z.s., ISSN 2571-3736. Dostupné z https://www.internetembezpecne.cz/internetem-bezpecne/malware/virus/

[16] Projekt Internetem bezpečně, Realizátorem projektu je nezisková organizace you connected, z.s., ISSN 2571-3736. Dostupné z https://www.internetembezpecne.cz/internetem-bezpecne/malware/virus/

[17] Správa sítě s.r.o., Správa sítě slovník pojmů. Dostupné z https://www.sprava-site.eu/ransomware

a praktickému přístupu k datům, souborům, aplikacím, prostě celému informačnímu systému v kostce z jakékoliv lokality či místa na světě, kde je dostupné internetové připojení. Vzdálená plocha vytváří prostředí uživatele jako by se nacházel na samotném zařízení (stolním počítači neboli desktopu).

Pachateli takto dochází typicky k připojení na zařízení (počítač nebo i mobil) poškozených, kde následně provedou např. přípravu transakcí v internetovém nebo mobilním bankovnictví a poškození následně transakce potvrdí dopsáním potvrzovacího kódu. Podstatné je, že i vzdálený přístup je možné provést přes VPN. Pachatelé používají často volně dostupné a stažitelné programy jako je ANyDesk, TeamViewer.[18]

Cookie / HTTP cookies – jsou data, která může webová aplikace uložit na počítači přistupujícího uživatele. Prohlížeč potom tato data automaticky odesílá aplikaci při každém dalším přístupu. Cookie se dnes nejčastěji používá pro rozpoznání uživatele, který již aplikaci dříve navštívil, nebo pro ukládání uživatelského nastavení webové aplikace. Dnes jsou často diskutovány v souvislosti se sledováním pohybu a zvyklostí uživatelů některými weby.[19]

Crack – je neoprávněné narušení zabezpečení ochrany programu nebo systému, jeho integrity nebo systému jeho registrace / aktivace.[20] Pro pochopení lze např. uvést soubory tzv. „cracky“ spouštěcích programů počítačových her nebo jiných programů, kdy soubor, umožňuje obejít např. autorizovaný kód nebo přihlášení.

Cracker – je právě jednotlivec, který se pokouší získat neoprávněný přístup k počítačovému systému. Tito jednotlivci jsou často škodliví a mají prostředky, které mají k dispozici pro prolamování se do systému.[21]

---

[18] Správa sítě s.r.o., Správa sítě slovník pojmů. Dostupné z https://www.sprava-site.eu/informacni-system

[19] Str. 34 Výkladový slovník kybernetické bezpečnosti, Petr Jirásek, Luděk Novák, Josef Požár, Policejní akademie ČR v Praze, Praha 2015

[20] Str. 35 Výkladový slovník kybernetické bezpečnosti, Petr Jirásek, Luděk Novák, Josef Požár, Policejní akademie ČR v Praze, Praha 2015

[21] Str. 35 Výkladový slovník kybernetické bezpečnosti, Petr Jirásek, Luděk Novák, Josef

Cross-site scripting (XSS) – je útok na webové aplikace spočívající v nalezení bezpečnostní chyby v aplikaci a jejího využití k vložení vlastního kódu. Vložený kód se obvykle snaží získat osobní informace uživatelů, obsah databáze či obejít bezpečnostní prvky aplikace.[22]

Elektronická pošta (E-mail) – je textová, hlasová, zvuková nebo obrazová zpráva poslaná prostřednictvím veřejné sítě elektronických komunikací, která může být uložena v síti nebo v koncovém zařízení uživatele, dokud ji uživatel nevyzvedne.[23]

Emailová hlavička – je část emailové zprávy, která obsahuje informace vázané k emailu, např. IP adresu odesílatele, historii pohybu zprávy, časy odeslání, doručení apod. Pro její zobrazení je však nutné email stáhnout (zajistit) ve správném formátu, např. .eml, aby se email stáhl celý, nejen text emailu. Emailovou hlavičku poté můžeme zobrazit tak, že otevřeme email (nejčastěji v Outlooku) a klikneme na „soubor“ – „vlastnosti“ – kde dole je „internetové záhlaví“, což jsou právě požadované informace.

2.1.2 Pojmy související s kybernetickou kriminalitou

Kybernetická kriminalita – viz kapitola 2.2 – popis kybernetické kriminality

Digitální stopa – viz kapitola 2.2.2 – specifika kybernetické kriminality

Sociální inženýrství – je způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace.[24] V rámci kybernetické kriminality se jedná o velmi využívaný způsob získání různých informací, od přístupů do zařízení

Požár, Policejní akademie ČR v Praze, Praha 2015

[22] Str. 36 Výkladový slovník kybernetické bezpečnosti, Petr Jirásek, Luděk Novák, Josef Požár, Policejní akademie ČR v Praze, Praha 2015

[23] Str. 44 Výkladový slovník kybernetické bezpečnosti, Petr Jirásek, Luděk Novák, Josef Požár, Policejní akademie ČR v Praze, Praha 2015

[24] Str. 107 Výkladový slovník kybernetické bezpečnosti, Petr Jirásek, Luděk Novák, Josef Požár, Policejní akademie ČR v Praze, Praha 2015

(instalace aplikace AnyDesk), po přesvědčení poškozených, aby požadovaný úkon provedli sami.

Útoky sociálního inženýrství využívají lidské zranitelnosti, emocí, zejména:

- *Strach a časový nátlak*: Lidé obecně jednají pod vlivem strachu a časové tísně neadekvátně. Například paradoxně čím více peněz na účtu máte, tím, je větší pravděpodobnost, že o ně přijdete, protože na Vás vliv strachu působí daleko více.
- *Reciprocita* – Lidé mají tendenci oplácet laskavost a útočníci tohoto využívají. Například pomoc kamarádům a příbuzným v tísni, falešné sbírky apod.
- *Závazek a důslednost* – Pokud se lidé zavážou k myšlence nebo cíli (ústně nebo písemně), je pravděpodobnější, že tento závazek dodrží, zejména pokud se s ním ztotožní.
- *Sociální přizpůsobení* – Lidé budou dělat věci, které vidí dělat ostatní. Zde mají obrovský vliv například falešné komentáře a recenze, nebo doporučení přátel.
- *Autorita* – Lidé mají tendenci podlehnout autoritám.
- *Chamtivost, pocit výjimečnosti a nedostatku* – Lidé ze své podstaty chtějí mít více, proto spojení slov „výhodné, exkluzivní, jen pro Vás“ způsobí, že lidé přestanou myslet do důsledku a je snadné je přesvědčit o nutnosti provedení nějakého úkonu.[25]

Blagging – metoda, která využívá sociálního inženýrství tzv. CEO – Command Executive Order – jde o fiktivní příkaz oprávněného k provedení nějaké činnosti, v tomto případě platby na účet. Tyto typy podvodů jsou ve většině případů vytvořeny na základě velmi dobrých znalostí trhu, struktury a zákazníků dané společnosti. Získané informace bývají zneužívány k přesvědčivé argumentaci, aby byly oběti snáze zmanipulovány k provádění požadovaných aktivit. Jedním z typických scénářů je, že se pachatelé pro navázání kontaktu vydávají např. za ředitele firmy

[25] Intranetové stránky ÚSKPV PP, metodika kybernetické kriminality

(např. prezident, CEO, CFO) nebo důvěryhodného partnera (např. právníci, notáři, auditoři, účetní atd.) společnosti. Pod touto záminkou pak kontaktují konkrétního zaměstnance firmy s tím, že byli kontaktováni např. výkonným ředitelem ve věci splatnosti nějaké pohledávky či uzavření smlouvy a přimějí tak zaměstnance firmy k žádoucí interakci.[26]

Phishing – je v širším pojetí podvodný způsob získání citlivých informací, dat nebo přístupu do nějakého systému prostřednictvím e-mailu, textových zpráv nebo telefonu (podle toho rozlišujeme Vishing a Smishing). V užším pojetí se jedná o útok vedený skrze elektronickou poštu nebo sociální sítě, zprávy. Pachatelé se obvykle vydávají za legitimní uživatele s cílem přimět svou oběť ke:

- Sdělení citlivých informací (k intern. bankovnictví, přihlášení k účtu).
- Přesměrování na podvodnou phishongovou stránku.
- Zaplacení smyšlených dluhů, smluvních závazků.
- Stažení škodlivého softwaru (programu, doplňků).

Při komunikaci používají pachatelé často některý ze způsobů zastření identity odesilatele:

a) *Napodobení adresy oprávněného uživatele* – tj., že emailová adresa se na pohled tváří, jako regulérní adresa odesilatele, ale ve skutečnosti není.
b) *Spofing adresy odesilatele* – email vypadá jako by byl odeslán legitimní (správnou organizací), ale název domény je odlišný. Například jako Netflix, ale pokud umístíte ukazatel myši na „Odesílatel“, uvidíte, že email přišel z adresy netflix@gmail.com.
c) *Infiltrace schránky skutečného odesilatele* – tato metoda je nejhůře odhalitelná, k odeslání emailové zprávy byla využita skutečná adresa odesilatele, pravděpodobně došlo k nabourání do schránky. Nebezpečí v tomto případě spočívá i v možnosti navázání komunikace na

[26] Policie ČR, Policie ČR. Dostupné z https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

předchozí relace, které si může pachatel nastudovat a napodobit tak styl písemného projevu.[27]

Pharming – je sofistikovanou verzí phishingu. Jedná se o útok na DNS server, na kterém dochází k překladu doménového jména na IP adresu. K tomu dojde, když poškozený zadá na internetovém prohlížeči internetovou adresu, na níž se chce připojit. Nedojde ale k připojení na skutečnou adresu, ale podvrženou, dojde k přesměrování. Můžeme rozlišit mezi tím, zda dojde k napadení zařízení u poškozeného nebo cílového serveru.[28]

Vishing – je typem phishingového útoku, jehož podstata spočívá v podvodném telefonním hovoru. Cílem pachatele je zejména získání citlivých informací od oběti (například. jméno, rodné číslo, adresa bydliště, číslo bankovního účtu, číslo platební karty, přihlašovací údaje, apod.), nebo vmanipulování do určité situace (instalace programu na vzdálený přístup na plochu, odeslání finančních prostředků ze svého účtu). Útočníci se zpravidla maskují za jiné identity: pracovníky bank, technickou podporu softwarových společností, úředníky, policisty, prodejci, zástupce sázkových společností, apod. Útočníci mohou používat tak zvaný spoofing. Pachatel zde využívá sociálního inženýrství založeného na vyvolání pocitu strachu, nebo snadného finančního zisku. V některých případech může jí i o obrácený Vishing, kdy telefonováním reagujete na upozornění, nebo reklamní sdělení.[29]

Smishing (SMS phishing) – je typ phishingu založený na rozesílání SMS zpráv s úmyslem vylákat citlivé údaje, instalaci škodlivého obsahu na zařízení oběti, či zmanipulování oběti k nějaké činnosti. Ve většině případů je součástí SMS zprávy odkaz, který vede na webovou stránku, která se tváří, jako regulérní stránka, například banky.[30]

---

[27] Intranetové stránky ÚSKPV PP, metodika kybernetické kriminality

[28] Str. 40 Trestněprávní ochrana před kybernetickou kriminalitou, JUDr. Kolouch, JUDr. Volevecký, Praha 2013

[29] Intranetové stránky ÚSKPV PP, metodika kybernetické kriminality

[30] Intranetové stránky ÚSKPV PP, metodika kybernetické kriminality

Spoofing (neboli „falšování“) – je prakticky nedílnou součástí online podvodů a podvodů využívajících prvky sociálního inženýrství, kdy se pachatel zastírá svou identitu nebo napodobuje identitu jinou. Zpravidla se jedná o identitu nějaké autority (např. státní instituce, banky, renomované společnosti, či konkrétního jednotlivce). Podstatné je, že poškozenému se zobrazí tel. Číslo opravdové (např. tel. Číslo banky nebo policie) tedy poškozený i když provede kontrolu, zda se jedná o správné tel. Číslo, nemá v tomto momentě možnost odhalit, že je jedná o pachatele trestné činnosti.

Druhy spoofingu

1) *Spoofing ID volajícího* – častým druhem spoofingu využívaným při vishingu je maskování čísla volajícího. Maskování může mít podobu čísla organizace, jednotlivce, konkrétního regionu apod. Jakmile dojde ke spojení hovoru, snaží se pachatelé získat citlivé údaje, čísla karet či přístup k bankovním účtům. Podobně může spoofing proběhnout u SMS zpráv. Pachatelé k zamaskování používají specializované online služby nebo aplikace.

2) *Spoofing e-mailové adresy* – emailová adresa u přijaté emailové zprávy je podvržená. V hlavičce emailu může být opravdová emailová adresa, ale není zřejmé, jestli pachatel znalý programování nemůže tyto informace pozměnit.

3) *Web spoofing* – falešné webové stránky odpovídající vzhledem původnímu webu nejčastěji bankám nebo jejich bankovnictví (zejména u smishingu). Tyto nápodoby mají za cíl získání hesel a přístupových údajů, případně čísel platebních karet. U většiny je při podrobném pohledu patrná odlišnost v URL adrese. Nicméně v dnešní době jsou i domény, které nabízejí zkrácení, případně změnu URL adresy, tedy je na místě otázka, jakým způsobem poté dojde ke změně.

4) *DNS spoofing* – DNS spoofing často úzce souvisí s web spoofingem. Útočníci ovlivní DNS cache na straně zařízení oběti tak, aby se při zadání konkrétní adresy zobrazila podvodná stránka. Technologie DNS totiž zjednodušeně řečeno slouží právě k přiřazení správných stránek ke správným adresám. Útočníci k ovlivnění DNS záznamů na koncovém zařízení používají specializovaných virů – malwaru.

5) *GPS spoofing* – nepříliš častá metoda, kde se jednotlivci mohou snažit maskovat svou GPS polohu. Zařízení má díky tomu pocit, že je na jimém místě než-li je. Podobný typ útoku je možné použít např. ke zmatení dronů navigovaných GPS apod.

6) *ARP spoofing* – síťový protokol ARP (Address resolution protocol) slouží k překladu adres síťové vrstvy (IP) na adresy spojové vrstvy (MAC). Útočník v případě ARP spoofingu provede tzv. Man-in-The-Middle (MiTM) útok, kdy odchytává pakety komunikace v síti a dokáže ji nejen odposlouchávat, ale i měnit.[31]

Vzdálený přístup – tento typ podvodného jednání spočívá v manipulaci poškozených (většinou za využití sociálního inženýrství), aby si do zařízení nainstalovali aplikace ke vzdálenému přístupu. Pod záminkou např. telefonátu podvodného bankéře, nabídky výhodné investice, falešné technické podpory využije pachatel poté program pro vzdálený přístup (AnyDesk, TeamViewer), přihlásí se do zařízení poškozeného, kde následně může provádět změny a ovládat zařízení poškozeného. Zajímavostí může být připojení u případů, kde se na svém zařízení přihlásí poškozený do svého internetového bankovnictví, kde poté pachatel provádí zadávání platebních příkazů. Ve vyžádaných informacích poté vystupuje zejména IP adresa poškozeného, k pachateli jsou pouze data spojená s aplikací na vzdálený přístup. Nicméně tyto data za sebou mnohdy pachatelé smazávají nebo promazávají.

Evropský vyšetřovací příkaz – je rozhodnutí justičního orgánu vydané či potvrzené justičním orgánem jednoho členského státu EU za účelem provedení vyšetřovacích úkonů v jiném členském státě EU s cílem shromáždit důkazy v trestních věcech.

Evropský vyšetřovací příkaz je založen na vzájemném uznávání, což znamená, že vykonávající orgán je povinen uznat žádost jiné země a zajistit její výkon. Příkaz je třeba vykonat stejným způsobem a za stejných podmínek, jako

[31] Intranetové stránky ÚSKPV PP, metodika kybernetické kriminality

by daný vyšetřovací úkon byl nařízen orgánem vykonávajícího státu. Evropský vyšetřovací příkaz lze též vydat za účelem získání již existujících důkazů.

Směrnice (Směrnice o evropském vyšetřovacím příkazu v trestních věcech č. 2014/41 EU) vytváří jednotný ucelený rámec pro získávání důkazních prostředků. Vyšetřovací úkony mohou zahrnovat například výslech svědků, telefonické odposlechy, skryté vyšetřování a informace o bankovních operacích.

Vydávající orgány mohou evropský vyšetřovací příkaz využít pouze v případě, je-li daný vyšetřovací úkon:

- *nezbytný,*
- *přiměřený a*
- *použitelný v obdobných vnitrostátních případech.*

Evropský vyšetřovací příkaz se vydává za použití standardního formuláře a je přeložen do úředního jazyka vykonávajícího členského státu EU nebo do jiného jazyka určeného vykonávajícím státem.[32] Policejní orgán tímto způsobem získává informace pro trestní řízení, žádá jej prostřednictvím státního zástupce.

2.1.3 Orgány a instituce související s prověřováním a vyšetřováním kybernetické kriminality

Mimo policejní orgány, státní zastupitelství a některé dotčené orgány státní správy v rámci kybernetické kriminality vystupují, či mohou vystupovat:

Národní bezpečnostní úřad (NBÚ) – je bezpečnostním orgánem České republiky, který se zabývá zejména ochranou utajovaných skutečností a státního tajemství. Mezi jeho úkoly patří také ochrana kybernetického prostoru a prevence kybernetických hrozeb v rámci státní správy a dalších institucí.

Konkrétně se NBÚ podílí na zajišťování bezpečnosti informačních technologií v rámci vládních organizací a dalších orgánů veřejné správy. Poskytuje také bezpečnostní certifikace a školení v oblasti kybernetické bezpečnosti a informačních technologií.

V souvislosti s kyberkriminalitou má NBÚ roli především v oblasti prevence

[32] European e-justice, European e-justice. Dostupní z https://e-justice.europa.eu /92/CS/european_investigation_order_mutual_legal_assistance_and_joint_investigation_teams

a ochrany kritické infrastruktury, která je klíčová pro stabilitu a bezpečnost státu a jeho občanů. Dále spolupracuje s dalšími bezpečnostními složkami, jako jsou policie, tajná služba a další orgány veřejné správy, při odhalování a stíhání kybernetických trestných činů.[33]

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) – je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku veřejně regulované služby v rámci družicového systému Galileo (to je evropský autonomní globální družicový polohový systém, který financuje Evropská unie).[34]

Úřad pro ochranu osobních údajů (ÚOOÚ) – je hlavní orgán státní správy v oblasti ochrany osobních údajů. Jeho úkolem je dohlížet na dodržování zákonů o ochraně osobních údajů a řešit stížnosti od občanů.[35]

Ministerstvo vnitra (MV) – je odpovědné za zajišťování bezpečnosti státu včetně kybernetické bezpečnosti a podpora prevence kybernetických útoků.

Ministerstvo obrany (MO) – je odpovědné za ochranu obrany a bezpečnosti státu, včetně ochrany kyberprostoru.

Česká národní certifikační autorita (CZ.NIC) – je instituce odpovědná zajištění provozu a bezpečnosti informačního systému základních registrů, registru obyvatel, registru osob a registru práv a povinností.[36]

za správu a řízení národního internetového domény a zajištění bezpečnosti

---

[33] Národní bezpečnostní úřad, Národní bezpečnostní úřad. Dostupní z https://www.nbu.cz/cs/o-nas/

[34] Národní úřad pro kybernetickou a informační bezpečnost, Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z https://www.nukib.cz/cs/o-nukib/

[35] Úřad pro ochranu osobních údajů, Úřad pro ochranu osobních údajů. Dostupné z https://old.uoou.cz/pusobnost/ds-1269/archiv=0&p1=1059

[36] Správa národních registrů, Správa národních registrů, národní certifikační autority. Dostupné z https://www.narodni-ca.cz/

českého kyberprostoru.

Finanční analytický útvar (FAÚ) – od roku 1996 plní funkci finanční zpravodajské jednotky České republiky a je součástí celosvětové sítě finančních zpravodajských jednotek. V roce 2017 jako osamostatněný úřad s celostátní působností převzal veškerou činnost předchozího Finančního analytického útvaru, tehdejšího odboru Ministerstva financí.

FAÚ je po celou dobu své existence hlavním gestorem opatření zaměřených na prevenci a boj proti praní peněz, financování terorismu a šíření zbraní hromadného ničení v České republice.

Činnost a pravomoc FAÚ je vymezena zákonem č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů (AML zákon) a zákonem č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdních předpisů.

Finanční analytický úřad zajišťuje úkoly, které pro úřad vyplývají ze zvláštních právních předpisů pro boj proti legalizaci výnosů z trestné činnosti a financování terorismu, a ze zvláštních právních předpisů upravujících oblast uplatňování mezinárodních sankcí za účelem udržování a obnovy mezinárodního míru a bezpečnosti, ochrany lidských práv a boje proti terorismu, v návaznosti na opatření přijatá Radou bezpečnosti OSN a orgány Evropské unie (dále jen „mezinárodní sankce“).

- Provádí sběr a analýzu údajů o podezřelých obchodech a provádí další úkony, které z analýzy vyplývají.
- Zajišťuje výkon koncepční činnosti v oblasti své působnosti, zpracovává komplexní návrhy na rozvoj a dotváření systému opatření proti legalizaci výnosů z trestné činnosti a financování terorismu a pro oblast uplatňování mezinárodních sankcí v celostátním i mezinárodním kontextu.
- Zpracovává v oblasti své působnosti návrhy zákonů a prováděcích předpisů, včetně jejich harmonizace s právními předpisy Evropské unie (EU) a přípravy pozic České republiky k návrhům nových předpisů a dalších dokumentů EU.

- Podílí se na tvorbě právních předpisů EU.
- Spolupracuje v oblasti své působnosti s mezinárodními organizacemi, s orgány se stejnou věcnou působností jiných států, s ústředními správními úřady a s právnickými osobami, Policie ČR, zpravodajské služby.
- Vydává v rozsahu své působnosti rozhodnutí ve správním řízení podle zvláštních právních předpisů a zastupuje úřad v soudním řízení správním.
- Zajišťuje a vykonává školení v oblasti své působnosti.

Oprávnění FAÚ jsou přesně definována v zákoně č. 253/2008 Sb. V tomto zákoně jsou definována základní oprávnění úřadu a v návaznosti na toto nejsou vyloučena ani oprávnění definována jinými právními předpisy.

Kontrola činnosti FAÚ je ze strany Poslanecké sněmovny Parlamentu ČR. Poslanecká sněmovna k tomu zřídila zvláštní kontrolní orgán a to „Stálou komisi pro kontrolu činnosti FAÚ“.[37]

V rámci PČR mají v prověřování a vyšetřování kybernetické kriminality svou podstatnou roli tyto součásti:

Národní centrála proti terorismu, extremismu a kybernetické kriminalitě SKPV (NCTEKK) – vznikla 1.1.2023 vyčleněním sekcí terorismu, extremismu a kybernetické kriminality z Národní centrály proti organizovanému zločinu služby kriminální policie a vyšetřování do nového samostatného útvaru s celostátní působností. NCTEKK je gestorem:

- metodického vedení v oblasti kybernetické kriminality,

- je Národním kontaktním místem pro kybernetickou kriminalitu v rámci uchování dat (tzv. "data freezing") na žádost České republiky, která se nacházejí na území cizího státu

- plní úkoly v rámci tzv. "emergency případů", tj. vyžadování dat, která se

[37] Finanční analytický úřad, Finanční analytický úřad. Dostupné z https://fau.gov.cz/o-uradu#kdo-jsme-a-co-delame

nacházejí na území cizího státu ve velmi naléhavých případech (např. důvodné podezření na ohrožení života).[38]

Útvar zvláštních činností služby kriminální policie a vyšetřování (ÚZČ SKPV) – je útvarem Policie České republiky, který v souladu s příslušnými ustanoveními trestního řádu, zákona o Policii České republiky a dalších právních předpisů provádí ve prospěch oprávněných bezpečnostních subjektů:

- sledování osob a věcí a další specializované úkony,
- odposlech a záznam telekomunikačního provozu (kompletní spolupráce s mobilními operátory na území ČR (výpisy z telekomunikačního provozu, dohledávání a zjištění IMEI, IMSI, čísla SIM apod.),
- uchování dat (tzv. "data freezing" – uchování dat dle § 7b tř.) a následné vyžádání těchto dat u mobilních operátorů na území ČR.
- zjišťování informací z datového provozu (spolupráce se zahraničními a českými poskytovateli, výpisy z datového provozu, dohledání IP adres, logů, apod.),
- uchování dat (tzv. "data freezing") u poskytovatelů na území ČR a následné vyžádání těchto dat,
- zajištění komunikace v e-mailových a datových schránkách,
- Emergency (data, která se vyžadují na území ČR).[39]

Úřad služby kriminální policie a vyšetřování Policejního prezidia – se zabývá metodikou, podporou výkonu služby a koordinační činností po linii tzv. ostatní kriminality páchané v kyberprostoru - tj. "běžnou" kriminalitou, jejíž existence není primárně závislá na existenci "kyberprostoru" (jako podvody, vydírání, vyhrožování, pornografie atp.) ale ve svých specifických projevech je v kyberprostoru páchána, anebo její páchání moderní technologie usnadňují. Poskytuje podporu v oblastech:

- hospodářské a majetkové kriminality (e-podvody, scamy, phishing, sociální inženýrství, investiční podvody a podvody s kryptoměnami),

[38] Intranetové stránky ÚSKPV PP, metodika kybernetické kriminality
[39] Intranetové stránky ÚSKPV PP, metodika kybernetické kriminality

- mravnosti a mládeže (pornografie, sextortion, dětská pornografie)
- násilí a občanského soužití (vydírání, výhružky),
- postupy základů zajišťování elektronických stop,
- e-maily, komunikační platformy jako Facebook, Whatsapp atp., ohledání elektronických zařízení,
- Informace k nejnovějším trendům kriminality,
- Jazykové mutace poučení,
- Diskuze (zde lze uvést konkrétní problém nebo dotaz, kdy na něj poté odpoví osoby, které se buď s daným problémem již setkaly, nebo pomohou naznačit směr postupu).

Na intranetových stránkách ÚSKPV PP je v rámci metodiky poskytováno nejen vysvětlení některých pojmů, postupů u prověřování, vyžadování informací, provádění úkonů, ale také jsou zde k dispozici již vytvořené Koordinační přípisy (ty obsahují informace zejména k rozsáhlé trestné činnosti za účelem zefektivnění a usměrnění postupu).[40]

2.2 Popis problematiky kybernetické kriminality a jejích specifik

Kybernetická kriminalita (označována také jako „Cyber crime“) je trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti.[41]

Kybernetická kriminalita je tedy kriminalita, kde jsou prostředky informačních technologií:

[40] Intranetové stránky ÚSKPV PP, metodika kybernetické kriminality

[41] Str. 69 Výkladový slovník kybernetické bezpečnosti, Petr Jirásek, Luděk Novák, Josef Požár, Policejní akademie ČR v Praze, Praha 2015

a) *použity jako nástroj pro spáchání trestného činu* (např. vytvoření podvržených internetových stránek internetového bankovnictví, kde po přihlášení pachatelé získají přístupové údaje, jenž použijí k získání finančních prostředků),
b) *jsou cílem útoku pachatele, přičemž tento útok je trestným činem* (např. data nějaké organizace či osoby),

za podmínky, že jsou tyto prostředky užity či zneužity v informačním, systémovém, programovém či komunikačním prostředí.[42]

Základní metodika prověřování kybernetické kriminality

KRIMINÁLNÍ SITUACE – je tvořena zejména úrovní rozvoje informačních a komunikačních technologií, úrovní užívaného zabezpečení, možnostmi a prací justičních a kontrolních orgánů.

TYPICKÉ ZPŮSOBY PÁCHÁNÍ – neoprávněné zásahy, změny v datech (vstupních, uložených, výstupních), neoprávněné pokyny k operacím, neoprávněné pronikání, napadení, využívání počítačového systému.

PACHATEL – buď samostatná jednotka (znalý problematiky nebo průměrný uživatel) nebo jako člen organizované skupiny, kde nižší člen nemusí mít znalosti z dané problematiky, plní jen úkoly dané mu znalým nadřízeným

MOTIV – primárně zisk, způsobení škody.

TYPICKÉ STOPY – počítačová neboli digitální stopa, věcné stopy, důkazy (zejména listinné), paměťové stopy (zejména poškozených, svědků).

TYPICKÉ VYŠETŘOVACÍ SITUACE – nejčastější je, že zjištěné skutečnosti nasvědčují tomu, že byl spáchán trestný čin, ale nedovolují možnost určení totožnosti pachatele.

ZVLÁŠTNOSTI PŘEDMĚTU VYŠETŘOVÁNÍ – podstatná část průběhu případu je spáchána v kyberprostoru, od toho se odvíjí možnosti důkazních prostředků a možnosti objasňování.

---

[42] Str. 12 Trestněprávní ochrana před kybernetickou kriminalitou, JUDr. Kolouch, JUDr. Volevecký, Praha 2013

ZVLÁŠTNOSTI PODNĚTU K VYŠETŘOVÁNÍ – primárně je podnět od poškozených, obětí, svědků (patrné jsou rozdíly ve znalostech IT mající vliv na množství získaných informací).

TYPICKÉ POČÁTEČNÍ ÚKONY A JEJICH ZVLÁŠTNOSTI – výslech poškozeného, svědka, zajištění komunikace, ohledání věci, vydání, předložení věci, zajištění finančních prostředků.

ZVLÁŠTNOSTI VYŠETŘOVACÍCH VERZÍ A ORGANIZACE VYŠETŘOVÁNÍ – podle způsobu spáchání a zásahu v kyberprostoru (podstatný časový faktor, po určité době dochází k zániku dat, možno sice použít freezing, vhodné a efektivní plánování vyšetřování je důležité pro objasňování této trestné činnosti).

ZVLÁŠTNOSTI NÁSLEDNÝCH ÚKONŮ, NÁSLEDNÉ ETAPY VYŠETŘOVÁNÍ – nejčastěji vyžadování informací, výslechy dalších osob, vyhodnocování získaných informací, odborná vyjádření, znalecké posudky, vypořádání zajištěných důkazních prostředků.

ZVLÁŠTNOSTI ZAPOJENÍ VEŘEJNOSTI DO VYŠETŘOVÁNÍ – veřejnost spolupráci obecně přijímá, byť přínos do daného případu může být rozdílný, podstatná je však prevence, osvěta veřejnosti.

2.2.1 Statistické údaje o kybernetické kriminalitě

Ministerstvo vnitra

Podle Zprávy o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky, z roku 2022 trestná činnost páchaná prostřednictvím internetu i jiných sítí zaznamenala v roce 2022 nárůst na 18 554 skutků (+ 9 036 z roku 2021, tedy nárůst o +94,9 %). Nejčastěji byly tímto způsobem spáchány podvody mezi soukromými osobami (7 727, +3 640, +89,1 %), neoprávněné opatření, padělání a pozměnění platebního prostředku (4 283, +3 783, +756,6 %), neoprávněný přístup a poškození záznamu v počítačovém systému a opatření a přechovávání přístupového zařízení a hesla (2 575, +893, +53,1 %). Potvrzuje se tak předpokládaný trend, a to postupný přesun trestné činnosti jako takové do kyberprostoru. Kriminalita páchaná v kyberprostoru tvořila v roce 2022 10,2 % celkové registrované kriminality.

Významný byl nárůst protiprávní činnosti typem tzv. „inzertních podvodů“. Dalším častým typem byly podvodné telefonáty, kdy se pachatelé vydávali za bankéře, finanční poradce a policisty. Setrvalým problémem je podvodné jednání typu romance scam, BEC a CEO útoky, inzertní podvody a podvody s legendou výhodných investic. Celou ostatní kriminalitou páchanou v kyberprostoru prostupuje větší a větší uplatnění kryptoměn, ať již jako nástroje k provedení platby či vyvedení prostředků získaných trestnou činností do zahraničí, nebo jako objektu krádeží či podvodných jednání.[43]

Policie České republiky

V rámci prověřování a vyšetřování se u PČR používá funkce „sledovaná událost“, kdy se případ spadající do určité oblasti označí příslušným zatržítkem. To se promítá nejen do statistik, ale dále se s touto informací pracuje (např. u kyberkriminality označené „IT kriminalita“ se provádí zjišťování, zda případ nespadá do nějaké sériové trestné činnosti, toto provádí většinou oddělení analytiky a kybernetické kriminality, ale jejich výstup je dobré si dále prověřit např. v IS CDO a provést komunikaci s příslušným zpracovatelem). Jak bylo uvedeno, je tato funkce využitelná pro statistické výstupy, pro představu nárustu kybernetické kriminality byla z dat z tohoto systému vytvořena tabulka č. 1.

V této tabulce není patrné, jakou má kybernetická kriminalita objasněnost, pro vytvoření představy o objasněnosti byla zpracována data ze statistik kriminality Policie České republiky, které jsou k zobrazení na internetových stránkách Policie ČR. Z dat byly vytvořeny tabulky č. 2-4, v nichž jsou uvedeny nejčastější kvalifikace trestných činů v rámci kybernetické kriminality.

[43] Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky, v roce 2022, Ministerstvo vnitra ČR, str. 61

Tabulka 1

Množství skutků označených IT kriminalita (souhrn, tj. čj, přestupky, trestné činy) za časové období leden 2021–prosinec 2023 [44]			
Měsíc	rok 2021	rok 2022	rok 2023
Leden	1686	2486	3190
Únor	1535	2499	3025
Březen	1659	2689	3444
Duben	1680	2508	2689
Květen	1635	2331	2981
Červen	1394	2501	2777
červenec	1341	2595	2574
Srpen	1529	2862	3078
Září	1607	2877	2965
Říjen	1666	3048	4311
listopad	2304	2967	3736
prosinec	2313	2899	2922
celkem evidováno skutků	**20349**	**32262**	**37692**
z toho trestných činů	**10535**	**21478**	**22847**

V tabulce č. 2 zobrazena objasněnost u trestného činu Neoprávněný přístup a poškození záznamu v počítačovém systému, opatření a přechovávání přístupového zařízení a hesla (§ 230, 231, 232 trestního zákoníku). V tabulce č. 3 je zobrazena objasněnost u trestného činu Podvodu (§ 209 trestního zákoníku), kdy ale ve statistice není rozlišeno, jestli se jedná o klasický podvod nebo o IT kriminalitu. V tabulce č. 4 je poté zobrazena objasněnost u trestného činu Neoprávněné opatření, padělání a pozměnění platebního prostředku (§ 234 trestního zákoníku), zde také není rozlišeno, jestli se jedná o IT kriminalitu nebo běžný způsob spáchání. Data uvedená v tabulkách č. 2-4 jsou výtahem ze statistik kriminality Policie České republiky.[45]

[44] Zdroj informační systémy PČR ČR

[45] Policie České republiky, Policie ČR. Dostupné z https://www.policie.cz/statistiky-kriminalita.aspx

Tabulka 2

Objasněnost trestných činů 2021 - 2023 v ČR - Neoprávněný přístup a poškození záznamu v počítačovém systému, opatření a přechovávání přístupového zařízení a hesla (§ 230, 231, 232 trestního zákoníku				
rok	**měsíc**	**celkový počet skutků**	**množství objasněných skutků**	**objasněnost v procentech**
	leden	134	5	3,7%
	únor	268	16	6,0%
	březen	400	26	6,5%
	duben	537	35	6,5%
	květen	685	46	6,7%
	červen	823	60	7,3%
	červenec	960	65	6,8%
	srpen	1 112	81	7,3%
	září	1 284	102	7,9%
	říjen	1 419	110	7,8%
	listopad	1 603	130	8,1%
2021	prosinec	1 866	158	8,5%
	leden	249	3	1,2%
	únor	486	12	2,5%
	březen	671	21	3,1%
	duben	937	29	3,1%
	květen	1 247	47	3,8%
	červen	1 495	60	4,0%
	červenec	1 797	68	3,8%
	srpen	2 093	81	3,9%
	září	2 313	90	3,9%
	říjen	2 535	101	4,0%
	listopad	2 670	113	4,2%
2022	prosinec	2 848	127	4,5%
	leden	238	1	0,0%
	únor	468	9	1,9%
	březen	684	19	2,8%
	duben	848	32	3,8%
	květen	998	45	4,5%
	červen	1 143	54	4,7%
	červenec	1 260	62	4,9%
	srpen	1 400	72	5,1%
	září	1 512	80	5,3%
	říjen	1 625	88	5,4%
	listopad	1 794	103	5,7%
2023	prosinec	1 909	117	6,1%

Tabulka 3

Objasněnost trestných činů 2021 - 2023 v ČR - trestný čin Podvodu (§ 209 trestního zákoníku)				
rok	**měsíc**	**celkový počet skutků**	**množství objasněných skutků**	**objasněnost v procentech**
	leden	540	21	3,9%
	únor	1 081	70	6,5%
	březen	1 612	132	8,2%
	duben	2 149	223	10,4%
	květen	2 671	339	12,7%
	červen	3 252	483	14,9%
	červenec	3 723	563	15,1%
	srpen	4 213	666	15,8%
	září	4 785	790	16,5%
	říjen	5 385	924	17,2%
	listopad	6 084	1 047	17,2%
2021	prosinec	6 789	1 228	18,1%
	leden	950	53	5,6%
	únor	1 879	114	6,1%
	březen	2 861	194	6,8%
	duben	3 890	277	7,1%
	květen	4 881	417	8,5%
	červen	5 870	582	9,9%
	červenec	6 704	664	9,9%
	srpen	7 708	789	10,2%
	září	8 685	891	10,3%
	říjen	9 726	1 049	10,8%
	listopad	10 719	1 205	11,2%
2022	prosinec	11 658	1 345	11,5%
	leden	1 211	58	4,8%
	únor	2 291	91	4,0%
	březen	3 552	226	6,4%
	duben	4 466	361	8,1%
	květen	5 425	464	8,6%
	červen	6 409	580	9,1%
	červenec	7 325	673	9,2%
	srpen	8 475	775	9,2%
	září	9 436	880	9,3%
	říjen	10 650	1 042	9,8%
	listopad	11 754	1 305	11,1%
2023	prosinec	12 634	1 527	12,1%

Tabulka 4

Objasněnost trestných činů 2021 - 2023 v ČR trestný čin Neoprávněné opatření, padělání a pozměnění platebního prostředku (§ 234 trestního zákoníku)				
rok	**měsíc**	**celkový počet skutků**	**množství objasněných skutků**	**objasněnost v procentech**
	leden	298	27	9,1%
	únor	593	68	11,5%
	březen	910	161	17,7%
	duben	1 249	269	21,5%
	květen	1 684	356	21,1%
	červen	2 255	506	22,4%
	červenec	2 909	614	21,1%
	srpen	3 648	770	21,1%
	září	4 341	936	21,6%
	říjen	4 966	1 088	21,9%
	listopad	5 590	1 296	23,2%
2021	prosinec	6 107	1 513	24,8%
	leden	635	75	11,8%
	únor	1 256	166	13,2%
	březen	2 203	316	14,3%
	duben	3 133	454	14,5%
	květen	4 131	635	15,4%
	červen	5 161	826	16,0%
	červenec	6 275	971	15,5%
	srpen	7 367	1 179	16,0%
	září	8 426	1 381	16,4%
	říjen	9 584	1 531	16,0%
	listopad	10 688	1 745	16,3%
2022	prosinec	11 848	1 893	16,0%
	leden	1 296	55	4,2%
	únor	2 415	174	7,2%
	březen	3 519	355	10,1%
	duben	4 538	476	10,5%
	květen	5 570	646	11,6%
	červen	6 554	815	12,4%
	červenec	7 492	976	13,0%
	srpen	8 558	1 175	13,7%
	září	9 531	1 351	14,2%
	říjen	10 787	1 569	14,6%
	listopad	11 843	1 761	14,9%
2023	prosinec	12 802	1 952	15,3%

2.2.2 Kybernetická kriminalita jako součást kriminality

Kybernetická kriminalita je v současné době již nedílnou součástí celkové kriminality. Z tabulky č. 1 je patrné, že v posledních 3 letech došlo k výraznému nárůstu registrovaných skutků. V roce 2023 se může zdát, že nárůst byl zpomalen, ale to je dáno i tím, že dochází ke slučování novějších skutků se stále aktivními skutky z roku 2022 (v rámci sériové trestné činnosti). Zároveň je patrné, že ke snížení tohoto typu kriminality nedojde, pro pachatele je tento způsob páchání trestné činnosti lákavý, neboť má **pro pachatele zejména tyto pozitiva** (pro občany a policejní orgány se jedná o negativa):

- **Výhodný poměr nákladů a zisků** – náklady na páchání kybernetické kriminality nejsou vysoké (jsou vyšší u organizovaných skupin, kteří mají lepší vybavení a zabezpečení), pro standartní způsoby postačí běžný počítač, připojení na internet, mobilní telefon, doplňkové programy (na tvorbu malware, speciální prohlížeče, aplikace na spoofing) jsou převážně ke stažení na internetu, přičemž v poměrně krátké časové době lze od poškozených získat stovky tisíc nebo i miliony Kč, při vytrvalém a chytrém přístupu lze v řádu měsíců i od jednoho poškozeného získat několik milionů korun českých.
- **Snadná legalizace výnosu z trestné činnosti** – díky rychlému přístupu do bankovnictví, online směnáren, aplikací s kryptoměnou apod. lze výnos z trestné činnosti v rámci krátké časové doby (několika hodin nebo i minut, podle způsobu převodů finančních prostředků) nechat „procestovat“ několik bank, online směnáren či internetových prodejních míst (nejen s kryptoměnou, ale i doplňkovými produkty do počítačových her), čímž významným způsobem dojde ke ztížení vytrasování finančních prostředků nebo výnosu z trestné činnosti a zpomalení prověřování a vyšetřování. Dostatečným procesem legalizace již dokonce některá data nemusí být k dispozici.
- **Není nutný osobní kontakt s poškozenými** – jelikož kontakt probíhá většinou telefonicky, přes whatsapp nebo jiné komunikační aplikace, pachatel není v osobním kontaktu s poškozenými, čímž ve většině

případů odpadají některé možnosti identifikace (v úvahu přichází identifikace pomocí hlasu). U psaných textů je mnohdy zkreslena případná identifikace tím, že je pachatelem používán některý typ volně dostupného překladače pro překlad do jiného jazyka.

- **Možnosti překrývání, změn či mazání důkazních prostředků** – pachatelé využívají pro ztížení jejich vypátrání programy, aplikace, které jim dávají možnost *překrýt* (např. jejich telefonní číslo, kdy se poškozenému zobrazí telefonní číslo jiné), *změnit* (speciální internetové prohlížeče, programy, např. na změnu IP adresy), *smazat data* (např. v doručeném emailu pachatel promaže hlavičku, po vzdáleném přístupu smaže data, která se vztahují k jeho zásahu do počítačového systému, zařízení), čímž významným způsobem ovlivňují důkazní situaci v daném trestném činu. Tyto způsoby, programy jsou mnohdy běžně dostupné, nevyžadují schopnosti programování, pouze „naučení se pracovat“ s daným programem jako nástrojem. Při užití vhodných způsobů již dokonce vyžadovaná data nemusí být k dispozici.
- **Možnost použití služeb z různých států, zemí** – pachatel (v rámci ztížení svého dopadení) může využít služby (zejména telekomunikační a finanční) z různých zemí (např. telekomunikační služby Orange ve Francii, doménu registrovanou na Ukrajině, IP adresu registrovanou v Německu, online směnárnu v Singapuru apod.), kdy tímto rozčleněním ztíží prověřování trestného činu (je nutno vyžádat několik právních pomocí s tím, že každý stát reaguje jiným způsobem v jiné časové době).
- **Možnost páchat tuto trestnou činnost z kteréhokoli místa v jakýkoliv čas** – dle způsobu páchání činu je nutný pouze internet nebo telefonní připojení, lze tedy páchat z jakéhokoliv místa na zemi v jakoukoliv časovou dobu. Tímto způsobem, zejména ve spojením s využíváním služeb různých zemí, pachatel komplikuje své dopadení, hlavně když tím způsobí mezinárodní charakter daného trestného činu (např. z území jiného státu páchá trestnou činnost na území jiného státu).

- **Problematika propojení sériové trestné činnosti** – ve spoustě případů se podaří na základě shody v důležitých atributech (jako je doména, IP adresa, bank. účet) propojit jednotlivé případy do série, což se však nemusí podařit vždy, některé atributy (jako např. telefonní číslo) už sami o sobě k propojení případů stačit nemusí, je to dáno možnostmi překrytí, změny daného atributu, či získání přístupu do bankovnictví na darkwebu (tedy daný čin páchá poté jiná skupina).
- **Rozdíl v technologické a znalostní vyspělosti mezi pachateli, justičními orgány a poškozenými** – pachatelé jsou ve většině případů technologicky i znalostně vyspělejší, což jim dává velmi podstatnou výhodu, u policejních orgánů se situace v současné době zlepšuje, ale někdy je problém s přístupem některých policistů (na pochopení kyber. Kriminality a její správné prověřování je nutné znát alespoň základy moderních technologií, kdy se občas naráží na odpor z důvodu naučení se nových věcí, které můžou být pro někoho těžké na pochopení). U občanů, kteří se stávají poškozenými, jsou znalosti většinou také mnohem menší nežli u pachatelů, to pachatelům umožňuje dokonat své jednání. Osvěta, zejména pomocí médií napomáhá, aby občané byly opatrnější, ale díky zakrývacím způsobům pachatelů je pro občany těžké včas odhalit podvodné jednání.

Stejně jako u ostatních odvětví kriminality můžeme rozdělit kybernetickou kriminalitu na kriminalitu skrytou (latentní) a kriminalitu registrovanou. V latentní kriminalitě tohoto typu se nachází většinou kriminalita s nižší společenskou škodlivostí, zejména s nižšími škodami. Mnohdy sice dojde i ke zjištění některých těchto skutků, např. při vyhodnocení transakcí na bank. Účtu podezřelého, ale poškození mnohdy vzhledem k nízké škodě danou věc řešit vůbec nechtějí.

U škod nad desítky a zejména stovky tisíc korun českých nebo skutků s větší společenskou závažností (např. zakódování zdravotní dokumentace za účelem zaplacení za jejich rozkódování) poškození většinou oznámí daný trestný čin, v rámci něhož jim byla způsobena újma, po čemž následuje prověření věci policejním orgánem.

2.2.3 Specifika kyberkriminality

Jako každý typ kriminality, tak má i kyberkriminalita svá specifika, tj. odlišnosti, oproti jiným typům kriminality.

Základní specifika jsou tyto pojmy a možnosti:

a) *Digitální stopa*
b) *Metadata*
c) *Možnosti obstarávání prostředků k páchání kyber. kriminality*

Význačným specifikem je pojem „**digitální stopa**“, také označovaná jako počítačová stopa. Označení digitální stopa je však přesnější, jelikož se tato stopa nenachází jen na počítači, ale může se nacházet na mobilních telefonech, tabletech a dalších zařízeních. Tento pojem však není doménou jen kybernetické kriminality, ale vyskytuje se v současné době i v ostatních oblastech kriminality (zejména majetkové nebo násilné).

Pojem digitální stopa se vyznačuje narůstajícím významem, což je dáno novými způsoby páchání kriminality, kdy klasické kriminalistické stopy (daktyloskopické, trasologické, biologické, apod.) se v daných případech vyskytují jen sporadicky nebo vůbec a důkazních prostředků proti pachatelům je pomálu. Možnosti zkoumání digitálních stop jsou prostřednictvím OKTE, KÚ, či přibrání externího znalce, což je sice komplikovanější v tom, že jsou na externího znalce vynaloženy finanční prostředky navíc, ale z časového hlediska se jedná mnohdy o nejefektivnější způsob, jelikož zkoumání prostřednictvím OKTE trvá několik měsíců (až rok), jelikož jsou tyto součásti PČR zahlceny žádostmi o odborné zkoumání.

Digitální stopa je vymezena různými autory trochu odlišným způsobem:

Z **pohledu kriminalistiky**:

„*Počítačová stopa je informace nebo změna na materiálním nosiči, vzniklá v souvislosti s trestným činem, při jehož spáchání byla využita výpočetní technika,*

a která je zjistitelná a využitelná pomocí současných metod, prostředků, postupů a operací.“[46]

„*Počítačovou stopu lze charakterizovat jako změnu na nosiči informací, vzniklou v souvislosti s trestným činem, při jehož páchání byla použita výpočetní technika a která je zjistitelná za pomoci současných metod, prostředků a operací. Tyto stopy se nacházejí na pevném disku, vyměnitelných paměťových médiích, CD ROM, disketách atd.*“[47]

Z **pohledu informačních technologií** je digitální stopa souhrn různorodých záznamů o činnosti uživatele ve virtuálním prostředí. Je do dáno tím, že virtuální prostředí není anonymním prostorem. Každý uživatel zanechává v internetu určité informace (při prohlížení přes internet, vyhledání skrz Google, prohlížení Facebooku, nákupu zboží atd.). Jedná se o různorodé záznamy o činnosti uživatele ve virtuálním prostředí a právě soubor těchto informací se nazývá digitální stopa.

Záznamy o činnosti uživatele se uchovávají v zařízení, které užívá (počítač, mobilní telefon, chytré hodinky nebo chytrá televize) či jsou uchovávány v podobě např. příspěvků na sociálních sítích, prezentací prostřednictvím webových stránek, blogů, vlastních příspěvků do diskusí pod články, u internetových nákupů apod. V neposlední řadě je nutné uvést, že některé informace jsou internetem získávány „bez souhlasu“ uživatele.

Digitální stopu (z pohledu IT) uživatel vytváří veškerou svou činností ve virtuálním prostředí a tyto data jsou na internetu cenným artiklem, s nímž se dokonce obchoduje.

Rozdělení digitálních stop z pohledu IT:

a) **Vlastní** – jedná se o digitální stopu, kterou uživatel ve virtuálním prostředí zanechá vlastním přičiněním – vlastní činností.

a-a) Vědomá (aktivní) – je zanechaná cílenou a vědomou

[46] KONRÁD, Zdeněk, PORADA, Viktor, STRAUS, Jiří, SUCHÁNEK, Jaroslav. Kriminalistika, str. 342

[47] STRAUS, Jiří a kol. Kriminalistická metodika. Plzeň: Aleš Čeněk, 2006, s. 275.

činností (interakce na sociálních sítích, přispívání do diskusních fór, vkládáním fotografií do fotobank, mailová komunikace apod.

a-b) Nevědomá (pasivní) – vzniká jako vedlejší produkt tvorby vědomé digitální stopy. Ukládá se bez zásahu uživatele. Zpravidla se může jednat o informace z počítačového systému, počítačových sítí a užívaných online služeb (IP adresa, vyhledávané výrazy na internetu, údaje o stráveném času a činnosti na určité webové stránce (cookies), poskytovatel připojení, lokace apod.).

b) **Zanechaná přáteli** – mohou ji tvořit přátelé uživatele. Je to dáno tím, že ačkoliv uživatel může dbát na své soukromí, nelze se bezpodmínečně ubránit např. označení na fotografii na sociální síti nebo značení v příspěvku přítele. Ten v příspěvku dále může uvést geografickou polohu a označit další přátele, čímž se informace o soukromí uživatele (v tomto případě informace kde se nachází a s kým) může šířit i mimo okruh pečlivě zvolených přátel.

c) **Zanechaná nepřáteli** – tímto se označuje zanechání informací (ze strany „nepřátele uživatele“) o uživateli ve virtuálním prostředí, jenž je nepravda, jedná se o úmyslně zkreslenou informaci či jiným způsobem poškozuje dobré jméno uživatele. Je třeba si uvědomit, že jakékoliv informace vložené na internet již prakticky nelze vymazat.

Dále můžeme digitální stopy dělit na:

-Veřejné: informace, které dohledá kterýkoliv uživatel internetu

-Neveřejné: informace, které dohledá jen určitý okruh uživatelů internetu (přátelé na sociálních sítích, správci).

-Skryté: cookies a jiné technické záznamy o zařízení a připojení.[48]

Vlastnosti digitálních stop

[48] Projekt Internetem bezpečně, Realizátorem projektu je nezisková organizace you connected, z.s., ISSN 2571-3736. Dostupné z https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/

Digitální stopy se vyznačují několika typickými rysy, odlišnostmi ostatních typů kriminalistických stop, kterými jsou:

- Objemnost (velikost zajišťovaných dat může být od několika kB až po několik TB)
- Dynamičnost (schopnost změny digitální stopy) – nestálost, digitální stopa se v průběhu času může měnit (i v reálném čase např. u spoofingu)
- Umístění digitální stopy kdekoliv v kyberprostoru – umístění digitální stopy může být velmi důležité pro její dostupnost (dosažitelnost)
- Krátká životnost (dle typu digitální stopy) – některé digitální stopy můžou existovat několik měsíců (u zákonem upravených dob uchování dat, jako u IP adres), jiné pachatel může smazat záhy po skutku (např. komunikaci ve whatsappu)
- Proces zajištění, reprodukovatelnost

Mezi další specifika digitálních stop se řadí:

- nehmotnost digitálních stop,
- latentnost digitálních stop,
- manipulovatelnost s časem v počítačových systémech,
- způsob uchování záznamů,
- dynamika činnosti počítačových systémů,
- komplexnost prostředí,
- vysoký stupeň interní a externí interakce probíhajících procesů,
- velký geografický rozsah prostoru s digitálními stopami.[49]

Dokazování – elektronický důkaz

Společně s digitální stopou je nutné se zabývat jejím využitím jako důkazu, používá se pojem elektronický důkaz. Elektronický důkaz není v současné době jednoznačně definován. Obecně relativně přijímanou definici nabízí projekt „European Informatics Data Exchange Framework for Court and Evidence“, který označuje za elektronický důkaz „jakákoliv data, která jsou výstupem analogového

[49] PhDr. Marek Hejduk, MBA Policejní akademie České republiky v Praze Bezpečnostní teorie a praxe 1/2021 vědecký článek, str. 69-70

nebo digitálního zařízení potenciální důkazní hodnoty, která jsou generována, zpracována, uchována, nebo přenášena jakýmkoliv elektronickým zařízením“.[50]

Lze vycházet z § 89 odst. 2 trestního řádu „*Za důkaz může sloužit vše, co může přispět k řádnému objasnění věci*“. **Za elektronický důkazní prostředek lze považovat vše, co může sloužit jako zdroj relevantní informace a co je uchováno v elektronické podobě** – tedy především data. Data jako elektronické důkazní prostředky lze chápat jako nezpracovaná fakta a údaje bez přidané interpretace či analýzy. Samotné důkazy, tedy informace, jsou data, která byla interpretována tak, aby měla nějaký smysl pro jejich zpracovatele, resp. pro dokazování v trestním řízení[51]. Interpretování je nutné z toho důvodu, že ve svém základu jsou veškerá data zapsaná binárním kódem. Proto se také po zajištění zajištěná data opatřují kontrolním součtem, aby bylo možné doložit, že data nebyla v průběhu zajištění a zkoumání změněna.

Fáze zajišťování digitálních stop

Zajišťování digitálních stop zabezpečuje policista zpracovávající dané oznámení, a následně policista zařazený v organizačním článku útvaru, který vede trestní řízení. Digitální stopy se zajišťují převážně podle trestního řádu, a to předložením nebo vydáním věci (§ 78 tř.), odnětím věci (§ 79 tř). a ohledáním (místa činu, věci, dle § 113 tř).

Digitální stopy se zajišťují primárně:

- in natura jako digitální data uložená na hmotném nosiči (PC, notebook, server, USB flashdisk apod.) od dotčených subjektů (podezřelý, obviněný, svědek apod.)

- digitální data uložená na technologickém hmotném nosiči u Policie České republiky např. formou provedení bitové kopie nebo prostým zkopírováním digitálních dat (opatřené kontrolním součtem, jestliže je to v daném případě

[50] Atlas Consulting, člen skupiny Atlas Group, Právní prostor. Dostupné z https://www.pravniprostor.cz/clanky/trestni-pravo/elektronicke-dukazy-jako-vyzva-pro-trestni-proces

[51] Radim POLČÁK, František PÚRY, Jakub HARAŠTA a kol. Elektronické důkazy v trestním řízení, ISBN 978-80-210-8073-7, str. 94-95

možné),

- případně nasnímaná obrazovka monitoru pomocí softwaru, videí, fotografií, např. při zajišťování obsahu webových stránek, on-line komunikátorů, e-mailových zpráv.

Dalším specifikem kybernetické kriminality je výskyt a prověřování tzv. **metadat**.

Termín metadata lze vysvětlit jako data o datech. Jedná se o zvláštní druh dat, která mohou být rovněž součástí digitální stopy (z IT pohledu).

Každý soubor, který uživatel vytvoří, nese svá metadata – tabulku, informace, v nichž je zapsáno, kdy byl soubor vytvořen, kdy naposledy změněn a na základě registrace daných programů i kým byl vytvořen.

To samé platí i u pořizování fotografií, kde se metadata ukrývají v tzv. EXIF tabulce. Ta často navíc obsahuje i výrobce a model přístroje, jakým byla fotografie pořízena nebo GPS souřadnice místa stisknutí spouště.

I zaslaná mailová zpráva s sebou nese svá metadata v tzv. hlavičce mailu, kde se zapisuje např. IP adresa odesílatele a příjemce, ale i další důležitých serverů, kterými zpráva na internetu prošla.[52]

Možnost získání prostředků k páchání kybernetické kriminality

Mezi zásadní specifikum kybernetické kriminality lze zařadit možnosti získání prostředků potřebných pro její páchání. Díky digitalizaci a globálnímu propojení systémů a sdílení souborů, programů není nutné si fyzicky (osobně) obstarávat vybavení jako pro páchání např. při krádežích vloupáním (nástroje na překonání uzamčení, rukavice, čepice či kukly apod.). Vybavení (prostředky pro páchání trestné činnosti) lze rozdělit do 2 kategorií:

a) **hmotné** – mobilní telefony, notebooky, počítače, zázemí (prostory, odkud pachatelé páchají trestnou činnost),
b) **nehmotné** – programy, aplikace, softwarové vybavení.

[52] Projekt Internetem bezpečně, Realizátorem projektu je nezisková organizace you connected, z.s., ISSN 2571-3736. Dostupné z https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/

Hmotné vybavení je možné sehnat v běžných prodejnách, specifikum může být pouze výkon daného zařízení, který pachatelé potřebují (schopnější pachatelé si mohou vybavení kompletovat sami). V rámci prostor pachatelé využívají prostory běžně dostupné (byty, prostory pro firmy), které si pronajímají na falešná či skutečná jména či firmy zejména pocházející z ciziny. Při podezření na odhalení své působnosti se pachatelé přestěhují.

Nehmotné vybavení může být volně dostupné (na google play, či ke stažení na internetu – prohlížeč Tor, program na spoofing, Creations Tool pro vytvoření malware, AnyDesk) nebo se jedná o specifické programy nebo aplikace určené na protiprávní činnost, které jsou k dispozici na darknetu, či si je pachatelé vytvoří či upraví.

3 PRAKTICKÁ ČÁST

3.1 Příjem oznámení

Už při příjmu oznámení, v němž figurují informační a komunikační technologie, je nutné se zaměřit na některé informace, jež svojí podstatou jsou důležité pro řádné prověření věci. Tyto informace se můžou lišit dle způsobu spáchání jednotlivého skutku. Množství informací získaných v prvopočátku prověřování může zrychlit nebo zpomalit (pokud je jich málo) rychlost prověřování a vyšetřování. Vzhledem k tomu, že vyslýchaná osoba (ať už se jedná o oznamovatele, poškozeného nebo svědka) může mít malé nebo téměř žádné znalosti z informatiky, je mnohdy množství získaných informací a jejich kvalita, závislá na osobě provádějící výslech či poté přímo zajištění věci nebo dat. Jinými slovy je mnohdy nutné podrobnými otázkami z vyslýchané osoby doslova „vytáhnout“ informace, které vyslýchaná osoba často ani nepovažuje za důležité neboť dle jejího mínění nesouvisí s jejím případem, ale podrobným prověřením jednotlivých informací právě ona „nesouvisející informace“ může poskytnout vysvětlení důležitých skutečností pro řádné prověření trestného činu, které může vést i ke konkrétní osobě pachatele.

Co se týká jednotlivých úkonů, prováděných policejními orgány, tak ve většině zjištěných skutků bývá prvním úkonem nejčastěji výslech (konkrétně oznamovatele, poškozeného). Dále následuje zajištění důkazních prostředků od vyslýchaného, šetření ke zjištěným informacím, zajištění finančních prostředků, žádosti o informace (na základě souhlasu poškozeného, využití institutů dle § 8/2, § 88, § 88a trestního řádu) a další úkony, používané dle uvážení zpracovatele na základě zjištěných okolností.

Výslech

Výslechem je myšlen proces získání informací, zejména paměťových stop, z paměti vyslýchané osoby. Většinou se jedná o podání vysvětlení (dle § 61/1 zákona č. 273/2008 Sb. o Policii ČR, v případě, že se jedná o přestupkové jednání; dle §158/6 trestního řádu v trestním řízení). Ve výslechu je třeba, stejně jako u

každého výslechu, zodpovědět 7 kriminalistických otázek (KDO, CO, KDE, KDY JAK, ČÍM a PROČ, doplněno osmou otázkou s KÝM). Mimo běžné okolnosti je nutné se zaměřit na tyto skutečnosti a ve výslechu je přesně vymezit, zodpovědět (vycházejí z povahy kybernetické kriminality), jedná se o:

a) *Odhalení modus operandy* – zjistit jakým způsobem se pachatel dostal k poškozenému, jak získal jeho důvěru, jaký byl způsob komunikace, jak bylo s čím manipulováno (s finančními prostředky, zařízeními), apod., vhodné držet časovou osu skutku.
b) *Uvádět přesné názvy, případně i odkazy* na stránky/platformy/soc. sítě (známých platforem může stačit název (Facebook, Bazoš, Aukro...), u menších je potřeba zjistit celou adresu.
c) *Způsob komunikace* – email/Messenger (Facebook)/Instagram/sms zprávy, apod. – důležité pro další práci s komunikací, pokud je více druhů, uvést všechny – zjistit, odkud, kdo, kdy a s kým a jak komunikoval.
d) *Přesné časy komunikace/události* (zejména u telefonních hovorů)
e) *Přesné a jednoznačné názvy/identifikátory uživatelských profilů, emailů* (obou stran) – pozor na zobrazovaná jména a přezdívky. Nemusí jít o jedinečné názvy, typicky Facebook (Jan Novák není profil – jan.novak.967 už ano).
f) *Internetové připojení poškozeného* – důležité v případě narušení uživatelského účtu, nabourání do systému.
g) *Odkud poškozený komunikoval* – důležité pro určení místní příslušnosti.

Zajišťování důkazů

Vzhledem k tomu, že se ve většině případů jedná o informace, které jsou v digitálním prostředí, které je možné ovlivnit, jedná se často o neodkladné úkony, pachatel by s časovou prodlevou zajištění mohl některé důkazy smazat nebo změnit (např. smazat zprávy ve Whatsappu, změnit uložená data na zařízení).

Samotné zajištění je procesně možné několika způsoby, záleží na tom, co a kde se zajišťuje. Avšak v některých případech je možné se setkat s tzv.

„okresním právem“ (tzn. Že v různých částech naší republiky jsou jisté rozdíly ve zpracování či náhledu na nějaký aspekt či postup v řízení).

U případů, kdy oznamovatel zasílá oznámení elektronicky, se lze setkat s tím, že ke svému oznámení již připojí některé důkazy (komunikaci, výpisy z bank. Účtu). Na některých odděleních se ponechají přílohou k oznámení. Správný postup je zajištění dle trestního řádu – Oddíl čtvrtý: Zajištění věcí důležitých pro trestní řízení, primárně Zajištění věci pro důkazní účely – dle § 78 trestního řádu (Povinnost k předložení nebo vydání věci) a souvisejících ustanovení. Vhodné na komunikace, výpisy z bank. Účtu. V dalších případech zajištění důkazních prostředků se používá ohledání, dle § 113 trestního řádu (ohledání místa či věci).

To, jaký způsob zajištění je použit, je také závislé na tom, kdo zajištění provádí a co se zajišťuje. Zajištění dat specializovaným systémem provádí specializovaní pracovníci, většinou z oddělení analytiky a kybernetické kriminality, u složitějších případů je vhodné přibrat k ohledání či zajištění znalce z příslušného oboru (špatným zajištěním dat by mohlo dojít ke zničení nebo nepoužitelnosti dat jako důkazního prostředku).

Nejčastější důkazní prostředky:

Výpisy z bankovního účtu – poškozený může mít u sebe v papírové podobě nebo má v době oznámení stále fungující mobilní nebo internetové bankovnictví (v takovém případě je nutná rychlá dokumentace a poté blokace bankovnictví). Jsou nutné zejména pro posouzení možnosti zajišťování finančních prostředků.

Komunikace – jak bylo uvedeno, u některých druhů komunikace je předpoklad, že protistrana může komunikaci zablokovat nebo smazat profil, a tím se u některých platforem obsah znepřístupní (např. WhatsApp). Je tedy dobré provést alespoň rychlé snímky obrazovky s komunikací. Také je nutné nezapomenout zobrazit informace o protistraně komunikace nebo otevřít její profil a zadokumentovat jej.

E-mail – je nutné stáhnout v elektronické podobě přímo ze schránky uživatele. E-mailová zpráva obsahuje důležité informace (tzv. hlavičku), která se při tisku nebo screenshotu nezobrazuje. Pozor na přeposlané emaily, je nutné

zajistit původní email, při přeposlání dojde ke změně zápisu v hlavičce. V hlavičce emailu je zobrazena „historie“ pohybu emailu, tj. i přes jaké servery email prošel (POZOR zkušený pachatel je schopen hlavičku přepsat !!).

Sociální sítě, Profily – je nutné zjistit skutečné názvy profilů, udělat alespoň snímky obrazovky. Typicky na Facebooku "Martin Novák" je jen přezdívka, není jedinečná, vyhledáváním lze zjistit mnoho takových uživatelů. Skutečný název profilu je uveden například v adresní řádce a má obvykle tvar "martin.novak.976" – což je jedinečný údaj. Jistota je v případě facebooku ID profilu.

Facebook – archivace profilu může trvat i několik hodin, takže pokud se bude profil uživatele zálohovat, tak je výhodné už při příjmu oznámení spustit archivaci. Tento postup je pak vhodné poznamenat do protokolu o ohledání. POZOR, vytvořená záloha má platnost jen PĚT dní.

Inzertní portály – zajistit číslo inzerátu nebo jeho odkaz, případně uživatele, který inzerát podal. Lze fotograficky nebo stažením dat.

Pornografie – zajistit co nejdříve, je totiž předpoklad, že pokud je závadový obsah online, tak je vysoká pravděpodobnost, že bude odstraněn či znepřístupněn provozovatelem. U sdílení přes soc. sítě je nutné se zaměřit na to, kdo, co sdílel, komentoval atp. (opět pro minimální a rychlou dokumentaci lze použít snímky obrazovky). Dobré zajistit celý soubor, je možné pak zkusit prověřit metadata.

Soubory, dokumenty, složky – nejlépe zajistit původní, tedy nezkopírované soubory, v případě kopírování, vhodné provést bitovou kopii. Z metadat (zobrazují se např. ve vlastnostech) se zjišťují doplňující informace, např. typ fotoaparátu, lokalita, kde byla vytvořena fotografie, původce nějakého dokumentu apod., ale mnohdy tyto informace nejsou u souboru uvedena, jsou smazána nebo upravena (pachatel takto může učinit).

Zajištění finančních prostředků

V kybernetické kriminalitě je častým znakem způsobení finanční škody, kdy jsou peníze poškozených odeslány z jejich bankovních účtů na jiné bankovní účty nebo směnárny. Proto je častým úkonem zajištění finančních prostředků, primárně dle § 79a tř. (zajištění nástrojů a výnosů z trestné činnosti), provádí se Usnesením.

Někdy se lze setkat se zajištěním dle § 79g tř. Zajištění náhradní hodnoty (vychází z myšlenky smíchání původních finančních prostředků s jinými na bank. Účtu), ale vhodnější a používanější je postup dle § 79a tř.

Zajištění finančních prostředků se provádí na bankovních účtech, na které byly odeslány finanční prostředky poškozených. Je tedy nutné znát č. bank. Účtů, kam finanční prostředky byly přeposlány (např. z bankovního výpisu poškozených). Zajištění finančních prostředků by mělo být realizováno, pokud možno ihned po zjištění, že existuje možnost finanční prostředky získané trestnou činností zajistit, neboť postupně s ubíhajícím časem se zvyšuje pravděpodobnost, že pachatel peníze z cílové bank. účtu převede jinam nebo je vybere v hotovosti či jiným způsobem zužitkuje.

V praxi je možné zajišťovat jedním usnesením i vícero bankovních účtů, ale v případě stížnosti proti usnesení může nastat situace, kdy dojde ke zrušení usnesení a tím k odblokování zajištěných finančních prostředků. V mezidobí, než bude vydáno nové usnesení, tak může dojít k odčerpání původně zajištěných finančních prostředků. Řešení je jedním usnesením zajišťovat jeden bankovní účet. Toto řešení se může lišit (okresní právo).

Usnesení je nutné řádně odůvodnit, špatné odůvodněné usnesení může být důvodem pro jeho zrušení (v danou dobu je k dispozici výslech poškozeného, ten sám o sobě není dostatečný, je nutné jej zkombinovat s dalšími důkazními prostředky, jako výpis z účtu či jiný způsob jednoznačného určení cílového účtu a případné šetření k informacím zjištěným v daném stádiu). Dalším důvodem pro zrušení usnesení může být skutečnost, že v případě vydání usnesení bez předchozího souhlasu státního zástupce policejní orgán nezaslal ve stanovené lhůtě (48 hodin) ke kontrole státnímu zástupci (jedná se o nezhojitelnou procesní vadu).

Podmínky k použití Zajištění výnosů z trestné činnosti dle § 79a trestního řádu:

- *Lze pouze po zahájení úkonů trestního řízení dle § 158 odst. 3 tř.*, tedy pouze u TČ (u podvodu škoda nejméně 10000,- Kč)

- *Lze pouze na tuzemském bankovním u, nikoliv např. na bankovním účtu*

vedeném v cizině (níže rozepsány možnosti zajištění v cizině). Bankovní účet, na který byly trestným činem získány finanční prostředky, musí mít kód banky registrovaný zde v ČR,

- *Číslo cílového bankovního účtu musí být známo* (např. z výpisu) a okolnosti nasvědčují tomu, že předmětné peníze jsou nástrojem nebo výnosem z trestné činnosti (jinými slovy se musí jednat o peníze od poškozeného, ne někoho jiného, jinak by připadalo v úvahu zajištění finančních prostředků dle § 79g tř., Zajištění náhradní hodnoty).

- *Policejní orgán potřebuje k rozhodnutí o zajištění věci souhlas státního zástupce* (mimo standartní pracovní dobu jsou na OSZ zřízeny dosahy). Předchozího souhlasu není třeba v naléhavých případech, které nesnesou odkladu, což je v tomto případě splněno zejména tím, že časovou prodlevou dochází k dalšímu přečerpání, vybrání či jinému zužitkování finančních prostředků, proto je možné Usnesení vydat bez předchozího souhlasu státního zástupce (věc nesnese odkladu), ale poté je nutné Usnesení spolu s ostatními materiály do 48 hodin předložit příslušnému státnímu zástupci (ten buď vysloví souhlas nebo Usnesení zruší).

Pro vydání Usnesení o zajištění fin. prostředků na účtu není důležité, kdo je majitelem daného účtu.

Banka je povinna zajištění (musí se jí, co nejrychleji doručit, standartně datovou zprávou) realizovat neprodleně po doručení usnesení policejního orgánu dle § 79a odst. 1 tr. řádu, ať už byl dán předchozí souhlas státního zástupce či nebyl (primárním cílem je zajistit finanční prostředky na účtu v co nejbližší době, než je stačí pachatel z účtu odčerpat).

Při zajišťování finančních prostředků na účtu je vhodné spolu s usnesením v jedné zásilce zaslat stručnou žádost o sdělení výše zajištění, ale v poslední době již banky automaticky odpovídají s uvedením výše zajištěné finanční částky.

Jakmile banka doručí výši zajištění, je povinností zpracovatele zadat tuto hodnotu do záložky „Věc" v rámci daného spisového materiálu v IS ETŘ a dále tuto částku statisticky vykázat. Zapisuje se vždy SKUTEČNĚ ZAJIŠTĚNÁ

ČÁSTKA NA ÚČTU zaokrouhlená na celé koruny – tedy NE maximální výše zajištění.

Poté, co policejní orgán zjistí, kdo je majitelem účtu, na kterém byly zajištěny finanční prostředky, je nutné tomuto majiteli prokazatelně doručit dané usnesení o zajištění finančních prostředků (má právo na stížnost).

Zajištění finančních prostředků Finančním analytickým úřadem (FAÚ)

Ve specifických případech je možné provést zajištění finančních prostředků ve spolupráci s Finančním analytickým úřadem.

Jedná se o případy, kdy dojde k trestnímu oznámení o napadení bankovního účtu a převod peněžních prostředků a splňuje současně následující parametry:

a) jde o převod peněz, který není starší více jak 24 hodin – počítáno od posledního příkazu,

b) jde o škodu, která převyšuje 1.000.000,-Kč,

v případě, že je tato odčerpaná částka rozdělena do více debetních transakcí, pak je další podmínkou, aby alespoň jedna z těchto transakcí byla nejméně 500.000,-Kč ve prospěch jednoho bankovního účtu, částka 1.000.000,-Kč byla stanovena na základě rozšířené spolupráce mezi FAÚ a ÚSKPV ze strany FAÚ, a je třeba tuto hranici striktně dodržovat,

c) cílový účet je veden českou bankou (v případě států Evropské unie je možné věc konzultovat s pracovníkem ÚSKPV, v případě států ležících mimo Evropskou unii je snaha o zajištění finančních prostředků cestou FAÚ nerealizovatelná).

V případě, že oznámení splňuje podmínky, je ze strany policejního orgánu, který takové oznámení přijímal, kontaktován službu konající pracovník ÚSKPV z odboru hospodářské kriminality (dále jen "pracovník ÚSKPV"), který informaci od policejního orgánu převezme a vyhodnotí a bude-li splňovat výše uvedené parametry, předá informaci pracovníkovi FAÚ, za účelem provedení případných opatření v rozsahu zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. O tom, zda bude vyžádána

spolupráce s pracovníkem FAÚ vždy rozhoduje pracovník ÚSKPV.

Před informováním pracovníka ÚSKPV je třeba, znát tyto informace:

1) číslo jednací, pod kterým je předmětné trestní oznámení zpracováváno (v případě, že věc nesnese odkladu lze sdělit informace bez čísla jednacího, které pak bude pracovníkovi ÚSKPV sděleno dodatečně),

2) jméno, příjmení a datum narození poškozené osoby,

3) číslo napadeného bankovního účtu, popř. účtů,

4) číslo cílového bankovního účtu, popř. účtů,

5) konkrétní informace o předmětných peněžních transakcích (pokud jsou policejnímu orgánu v okamžiku předání informace známy), tyto by měly zahrnovat informaci o výši převedených peněžních prostředků, pokud byly peněžní prostředky odčerpány z napadeného účtu v několika transakcích, tyto transakce specifikovat, v případě, že poškozenému bylo napadeno vícero účtů, je třeba konkretizovat, jaká výše finančních prostředků byla z jakého bankovního účtu poškozeného odčerpána a na jaký cílový bankovní účet, popř. účty, byly předmětné transakce směřovány.

Po předání informací na FAÚ pracovník ÚSKPV následně podá zpětnou informaci prvotnímu policejnímu orgánu a to v rozsahu informací, které mu byly následně sděleny pracovníkem FAÚ. Zpravidla se jedná o informaci, zda na cílovém bankovním účtu (tj. bankovní účet, který byl užit pachatelem trestné činnosti ke shromažďování výnosů z trestné činnosti) byly zjištěny a následně blokovány finanční prostředky, v jaké výši, případně mohou být sděleny další informace o tom, jak bude dotčená banka ve věci nadále postupovat, tj. jaká opatření ve smyslu AML zákona budou bankou uplatňována. Zpravidla se jedná o postup banky v kontextu § 7, § 9, § 15 a § 18 zmíněného zákona.

Tento postup ale nijak nenahrazuje postup policejního orgánu po přijetí trestního oznámení, zejména postup dle ustanovení § 79a trestního řádu (zajištění nástrojů trestné činnosti a výnosů z trestné činnosti). Při zjištění, že peníze z trestné činnosti jsou na cílovém bank. Účtu, je nutné vydat usnesení

o zajištění finančních prostředků dle § 79a tř. a postupovat standartním způsobem (postup přes FAÚ zvyšuje šanci, že nedojde v mezidobí k jejich odčerpání, případně umožňuje získat představu o rozsahu, provázanosti s dalšími bank. účty).

Zajištění peněz u bank, institucí, majících sídlo mimo Českou republiku

V případě, že peníze byly přeposlány někam jinam nežli na bankovní účty v ČR, je postup složitější, zejména z důvodu vzájemného uznávání a použitelnosti trestněprávních předpisů naší republiky a cílového státu. To znamená, že možnost zajištění existuje, ale příliš se nevyužívá. Komplikace spojené s touto možností lze rozdělit do několika hledisek:

- **problém akceptování Usnesení o zajištění finančních prostředků** – některé instituce neakceptují rozhodnutí policejního orgánu, akceptují pouze rozhodnutí soudu, jiná neakceptují rozhodnutí orgánu ze zahraničí.

- **zpoždění mezi vydáním Usnesení a jeho realizací** – tím, že je nutné Usnesení doručit instituci v jiné zemi, nelze většinou (pokud nemá pobočku v ČR) doručit prostřednictvím datové schránky. Doručení prostřednictvím doručovací služby je příliš časově náročné. Variantou je emailové doručení, kde ale může být problém s ověřením doručení (varianta je nastavit si u emailu požadavek na potvrzení doručení).

- **provedení zajištění** – dotčená instituce buď provede zajištění nebo odpoví v případě vyskytnutí problému (např., že účet už neexistuje). Horší varianta je, když dotčená instituce nereaguje vůbec. Obecně ale lze říci, že komunikace tímto způsobem se postupně zlepšuje.

- **převod zajištěné věci do České republiky** – pro další rozhodnutí ve věci je dobré zajištěnou věc převést z cizí země do České republiky, ale je nutné brát v potaz práva osoby u níž byla předmětná věc zajištěna. Převod je nejčastěji proveden na základě rozhodnutí soudu (určení bank. Účtu a variabilního symbolu do soudní úschovy).

Ucelená metodika zajišťování v cizích zemích v současné době není, mnohé státy jsou sice schopny zajištění finančních prostředků akceptovat na

základě dobrovolnosti (po doložení oprávněnosti zajištění), tyto situace jsou vytvářeny na základě kontaktu policejního orgánu s jednotlivými organizacemi, firmami (možno využít ARO, ŘMPS). Případně mohou akceptovat rozhodnutí na základě vzájemného uznávání rozhodnutí justičních orgánů Pro další postup zpracovatele v takovém případě je důležité, jakým způsobem byly finanční prostředky z trestné činnosti legalizovány, lze vymezit několik způsobů převodů finančních prostředků:

- převody do banky jiné země nežli České republiky,
- přeshraniční platební převody (např. Wise, Western Union),
- převod platbami přes internet (platební brány, hlavně firmy registrované v cizích zemích),
- převod do kryptoměn
- nákup doplňků či rozšíření do počítačových her, programů.

Vypořádání zajištěných finančních prostředků

V případě zajištění finančních prostředků je nutné je vrátit oprávněné osobě. Vracejí se usnesením dle § 81a tř. za užití ustanovení § 80 a § 81 tř. nebo usnesením dle § 80 tř. (odlišnosti jsou dány okresním právem, § 81a tř. je na vrácení nehmotných a nemovitých věcí). Před samotným vrácením, vydáním zajištěných finančních prostředků je nutné si vyžádat předchozí souhlas státního zástupce ke zrušení, omezení zajištění dle § 79f. tř. (zrušení nebo omezení zajištění). Následně se vydá Usnesení dle § 79f tř. jímž se zruší zajištění finančních prostředků. POZOR na správný časový harmonogram, pokud nabyde právní moci usnesení o zrušení zajištění dříve (např. při podání stížnosti proti usnesení), nežli usnesení o vrácení věci, může nastat situace, kdy majitel účtu dojde do banky s usnesením o zrušení a bude požadovat zrušení zajištění, banka tedy zajištění zruší, ale peníze nebudou vráceny jiné osobě, jelikož usnesení o vrácení nenabylo právní moci. Situace by sice neměla nastat, banka by měla vyčkat pokynů policie, Vhodné je tedy vyžádat souhlas státního zástupce ke zrušení, omezení zajištění, poté vydat usnesení o vrácení, vydání věci a poté vydat usnesení o zrušení, omezení zajištění.

Určení osoby, které se finanční prostředky budou vydávat, je podstatným krokem před jejich vrácením. Standartně je možné je vrátit poškozené osobě, ale pokud peníze od poškozeného byly přeposlány na bank. Účet, kdy majitel účtu, na němž byly zajištěny finanční prostředky, uvede, že zajištěné prostředky (byť v částečné výši) jsou jeho majetkem a nikoliv poškozeného, nastává komplikace, kdy je nutné prokázat, kdo a případně v jaké výši má nárok na zajištěné finanční prostředky. Důkladným prověřením výpisů z bankovního výpisu je možné určit, zda peníze, které byly zaslány na bank. Účet např. byly obratem vybrány, přičemž v následné transakci byly připsány další peníze, ale ty už vybrány nebyly. Je tedy předpoklad, že se jedná o peníze osoby, od níž byly odeslány. Ale tato myšlenka nemusí být jednoznačným důkazem, že peníze lze vrátit dotyčnému poškozenému. V dané věci je také myšlenka, že peníze na bank. Účtu jsou „přisypány do měšce“, tedy nelze jednoznačně určit, čí a v jaké výši jsou. Vypořádání finančních prostředků tedy může být komplikací, protože v případě existence více poškozených, jenž si nárokují zajištěné finanční prostředky, je nutné (vyjma případů, kdy je zajištěna celá výše způsobené škody a lze vrátit peníze v plné výši každému poškozenému) určit jakým podílem se finanční prostředky budou vracet. V praxi opět platí okresní právo, kdy některé oddělení:

- určí samostatně na základě zjištěných skutečností, komu a v jaké výši budou finanční prostředky vráceny,
- vyžádají od místně a věcně příslušného soudu určení bank. Účtu a variabilního symbolu, kam následně převedou finanční prostředky a vrácení financí je poté řešeno v občanskoprávním řízení – vydání do soudní úschovy.

Správnějším postupem, v případě, že není možné vrátit finanční prostředky jednoznačně určené osobě (zejména v případě, že si na předmětné finanční prostředky dělá nárok více osob), je vydání do soudní úschovy (§ 80 odst. 1 tř. uvádí „*Není-li věci, která byla vydána nebo odňata, k dalšímu řízení už třeba a nepřichází-li v úvahu její propadnutí nebo zabrání, vrátí se tomu, kdo ji vydal nebo komu byla odňata. Jestliže na ni uplatňuje právo osoba jiná, vydá se tomu, o jehož*

právu na věc není pochyb. ***Při pochybnostech se věc uloží do úschovy a osoba, která si na věc činí nárok, se upozorní, aby jej uplatnila v řízení ve věcech občanskoprávních***“).

Vyžadování informací v jiných státech

V návaznosti na použitý způsob převodů je poté možno oslovit cílovou firmu (banku, směnárnu atd.) s žádostí o informace. Problémem je ale různá doba uchování dat v různých zemích. Toto zjištění informací je však pouze pro operativní účely, z procesního hlediska je potřeba vyžádat právní pomoc, jejíž vyřízení a odpověď na ní však trvá několik měsíců, oproti tomu přímo dotazované firmy odpoví mnohdy do několika dní. Lze však využít přímý dotaz na firmu se zdůvodněním ověření existence požadovaných informací a dat a poté po ověření jejich existence provést jejich freezing a pak vypracovat žádost na právní pomoc na jejich „získání“. Freezing se provádí cestou NCTEKK u států mimo ČR, v ČR se provádí cestou ÚZČ SKPV. Využívají se k tomuto žádosti v ETŘ, vzory jsou k dispozici na intranetu. Tam je k dispozici i seznam a zkušenosti s různými firmami a institucemi v cizích státech (jak odpovídají na žádosti, co je potřeba pro žádost apod.). K některým firmám postačí napsat email (datové schránky k dispozici nemají), jiné požadují vytvořit komunikační kanál pro ověření policejního orgánu (takto to má např. Binance.com). Komunikace však je nutná minimálně v angličtině (k tomu je v rámci operativního šetření možno využít překlady z oddělení policie zabývající se překlady z cizích a do cizích jazyků, lze je využít žádostí přes ETŘ).

Obecně se při vyžadování informací (zejména obsahující bankovní, osobní a podobné informace) postupuje dle **zákona č. 104/2013 Sb. o mezinárodní justiční spolupráci ve věcech trestních**, kde jsou stanoveny podmínky a okolnosti mezinárodní justiční spolupráce. Zde jsou uvedeny okolnosti ohledně právní pomoci a další podstatné skutečnosti vztahující se mezinárodní spolupráci a právům a povinnostem stran a osob. Dle tohoto zákona je možné vyžadování právní pomoci v cizím státu po splnění těchto podmínek:

1) *Vyžádat právní pomoc v cizím státu lze po zahájení úkonů trestního řízení a pro účely tohoto řízení.*

2) *Vyžádání právní pomoci v cizím státu* je možné pouze na základě žádosti státního zástupce a po podání obžaloby na základě žádosti soudu. To nevylučuje, aby státní zástupce z vlastního podnětu vyžádal právní pomoc i po podání obžaloby, jde-li o opatření důkazu, který potřebuje k zastupování obžaloby v řízení před soudem. Žádost o právní pomoc předloží státní zástupce Nejvyššímu státnímu zastupitelství, soud ministerstvu.

3) *Ústřední orgán žádost o právní pomoc přezkoumá* zejména s ohledem na podmínky a náležitosti vyplývající z tohoto zákona nebo mezinárodní smlouvy a na požadavky vyplývající z dosavadního vzájemného styku a zašle ji do cizího státu, pokud ji nevrátí spolu s uvedením důvodů, pro které ji nebylo možné do cizího státu zaslat. V souvislosti s přezkoumáním žádosti o právní pomoc může ústřední orgán požádat justiční orgán o nezbytné opravy a doplnění. Stanovisko ústředního orgánu je pro justiční orgán závazné.

4) *Justiční orgán může žádost o právní pomoc* a veškeré další písemnosti cizozemskému orgánu zaslat přímo pouze tehdy, umožňuje-li mezinárodní smlouva přímý styk justičních orgánů při uskutečňování právní pomoci.

Žádost o právní pomoc

Žádost o právní pomoc obsahuje zejména

a) označení justičního orgánu, který o právní pomoc žádá, a datum sepsání žádosti,

b) údaje o osobě, proti níž je vedeno trestní řízení,

c) popis skutku, jeho právní kvalifikaci s doslovným zněním ustanovení trestního zákona a popřípadě jiných právních předpisů,

d) přesný popis úkonu právní pomoci, o který je žádáno, včetně požadavků na způsob jeho provedení, a zdůvodnění potřeby jeho provedení.

K žádosti se připojí písemnosti a věci, které jsou potřebné k provedení požadovaného úkonu právní pomoci. Vyžadování právní pomoci probíhá prostřednictvím státních zastupitelství (policejní orgán vypracuje návrh či podnět

na vyžádání právní pomoci, který zašle dozorujícímu státnímu zástupci).

Použitelnost důkazů

V trestním řízení je samozřejmě potřeba správným způsobem procesně podchytit zjištěné informace, proto při operativním zjištění informací (prostřednictvím ARO, společných kontaktních míst apod.) většinou následuje podnět k vyžádání právní pomoci, kterým se procesně získají, zafixují, požadované informace. Mnohdy ale tento krok není potřeba, jelikož operativním šetřením nebyly zjištěny informace vedoucí ke konkrétní osobě, zejména když pachatel používá způsoby na překrytí, zamaskování svých původních (originálních) informací (své tel. Číslo, IP adresu) nebo požadované informace již nejsou k dispozici (např. u spoofingu, kdy informace u některých zahraničních společností jsou uchovávány jen několik týdnů či dnů). Dle zákona o mezinárodní justiční spolupráci ve věcech trestních platí, že:

- Justiční orgán může požádat, aby cizozemský orgán při provádění úkonu právní pomoci použil ustanovení právního řádu České republiky v rozsahu, v jakém to právní řád cizího státu umožňuje.
- Důkazy získané na žádost justičního orgánu cizozemským orgánem mohou být použity v trestním řízení v České republice, pokud byly získány v souladu s právním řádem dotčeného cizího státu, nebo v souladu s právním řádem České republiky.[53]

Mimo uvedený zákon je vhodné si ohledně dožadované země ověřit, jestli neexistují mezinárodní smlouvy, které by tento proces mohly významným způsobem ovlivnit (zejména zrychlit nebo zpomalit). U kybernetické kriminality se lze odkazovat na Úmluvu o počítačové kriminalitě (nejen v rámci Evropské unie), která upravuje zájmové oblasti trestního práva hmotného i procesního (je zde upraveno i urychlené uchování, zachování, zpřístupnění dat, prohlídky a zpřístupnění dat, apod.). V rámci zemí OSN je možné se odkazovat na Úmluvu

[53] Zákon č. 104/2013 Sb. o mezinárodní justiční spolupráci ve věcech trestních

OSN proti nadnárodnímu organizovanému zločinu č. 75/2013 Sb.m.s., jen je vhodné si ověřit, zda dožadovaný stát ratifikoval předmětnou úmluvu či mezinárodní smlouvu.

3.2 Možnosti prověřování a získávání informací

Podle množství informací, které je možno získat na počátku prověřování je potom vhodné si rozplánovat následující prověřování. V ETŘ je k tomuto dobré použít záložku u deliktu PLÁN PROVĚŘOVÁNÍ.

Jednotlivé informace lze vyhodnocovat prostřednictvím Oddělení analytiky a kybernetické kriminality (OAKK) nebo si zpracovatel může informace vyhodnotit sám. Tento postup je sice rychlejší, OAKK je většinou dost vytížené, tedy žádosti o spolupráci mohou být vyřízeny až po delší době, ale je závislý na schopnostech zpracovatele.

Pro získání a vyhodnocování informací lze použít volně dostupné zdroje (jsou využívány i OAKK) nebo policejní informační systémy. Na základě získaných informací je následně prováděno další zajišťování důkazních prostředků (žádosti o informace, výslechy, ohledání, vydání, předložení věci). Vyhodnocením dalších získaných informací se poté provádí další zjišťování informací a vyhodnocení, dle rozsáhlosti a komplikovanosti daného případu.

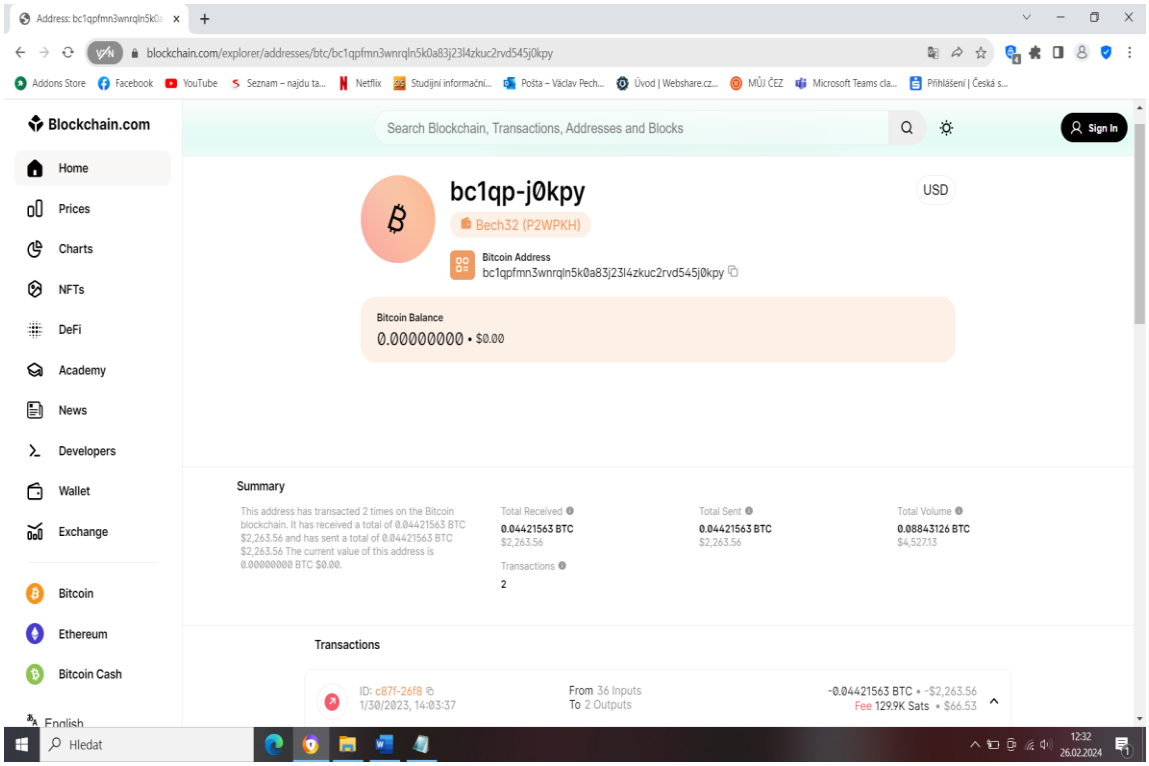
V rámci operativního zjišťování informací je možné použít i Národní centrálu proti organizovanému zločinu, odbor mezinárodní spolupráce, pracoviště ARO (to provádí zejména finanční šetření). Další informace lze zjistit prostřednictvím Útvaru zvláštních činností, Útvaru speciálních činností, při nejasnosti je nejlepší telefonická konzultace.

3.2.1 Otevřené (volně přístupné) zdroje

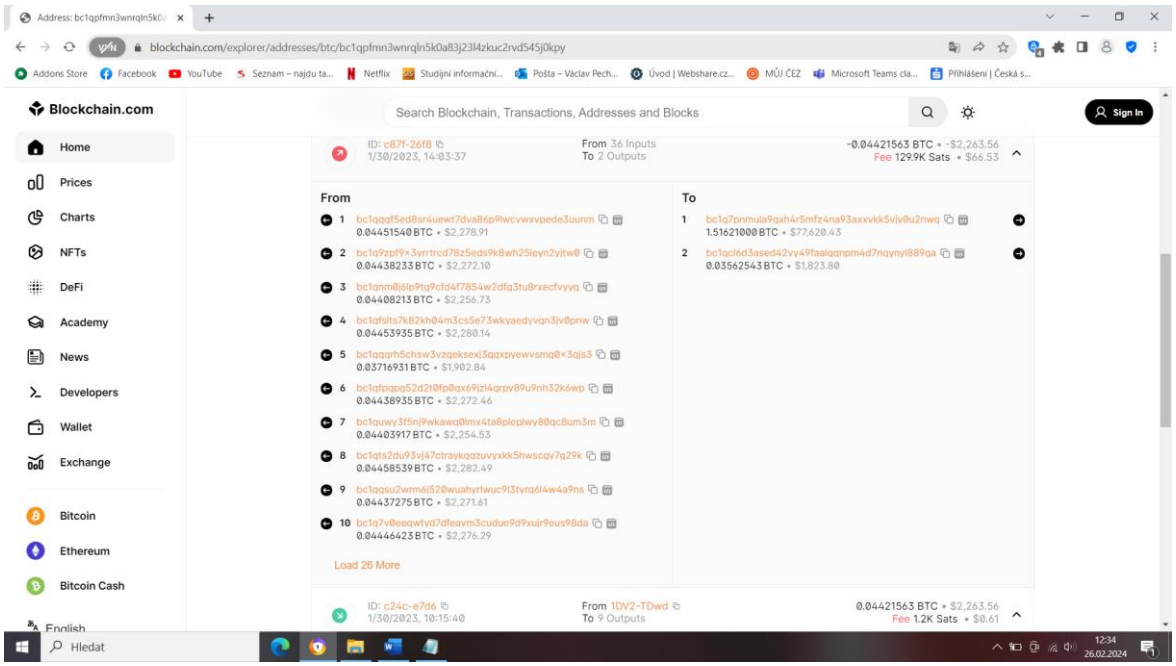
V dnešní době jsou k dispozici možnosti ověření některých informací i na běžném internetu. Na těchto internetových stránkách je možné získat informace, které lze využít pro zrychlení prověřování nejen kybernetické kriminality.

Blockchain.com (https://www.blockchain.com) – zde lze zadat

kryptoměnovou transakci a ověřit její „řetězení“, nechá se tedy provést šetření a zejména trasování kryptoměn, směrem k cílové kryptopeněžence. Na obrázku č. 2 je zobrazena ukázka lustrace bitcoinové adresy. Po srolování na dané stránce níže je zobrazen výčet transakcí navázaných k dané bitcoinové adrese (obrázek č. 3). Tímto způsobem lze provést šetření k různým kryptoměnám.



Obrázek 2 – ukázka lustrace bitcoinové adresy

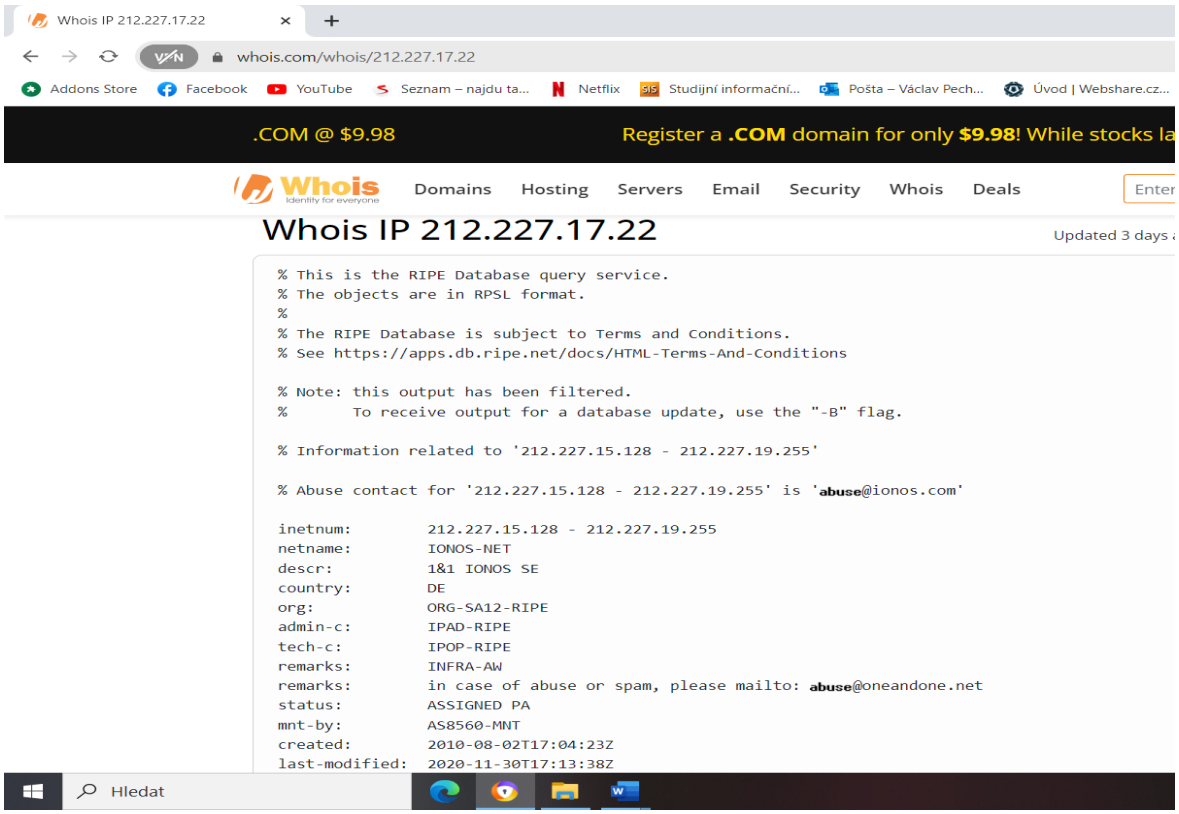


Obrázek 3 – provázané bitcoinové adresy s lustrovanou adresou

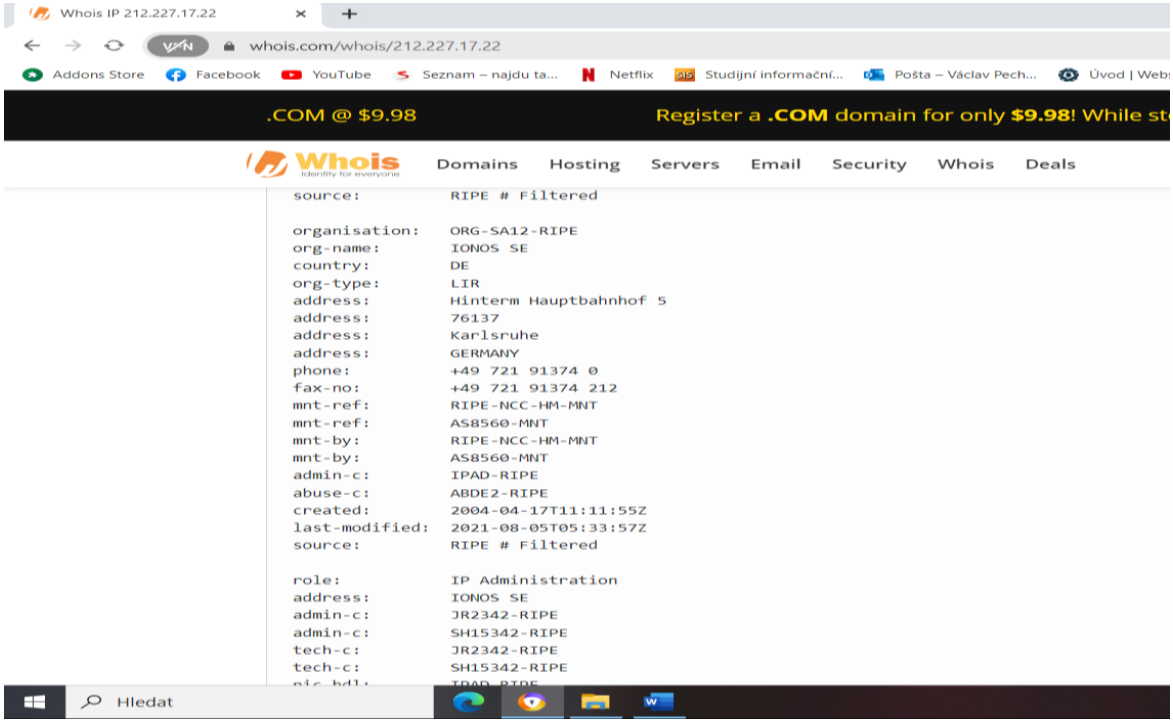
Whose is number (https://www.whoseno.com) – zde můžeme provést ověření telefonních čísel. Výhoda je možné nastavení předvolby, lze z různých zemí, bohužel vzhledem k množství existujících telefonních čísel mnohdy je lustrace negativní.

Ipqualityscore.com (https://www.ipqualityscore.com) – je internetová stránka, kde lze provést šetření k IP adresám, výhoda je, že rozlišuje i privátní IP adresy a VPN. Mimo jiné zde lze vylustrovat i email a telefonní číslo. V současné době vyžaduje při vyhledávání bezplatnou registraci, jinak je vyhledávání omezené (zejména množstvím dotazů).

Whois.com (https://www.whois.com) – zde lze provést šetření k doménám, IP adresám, emailům. Na obrázku č. 4 je ukázka lustrace IP adresy. Na obrázku č. 5 je druhá část ukázky lustrace IP adresy, zobrazené údaje o registrátorovi.

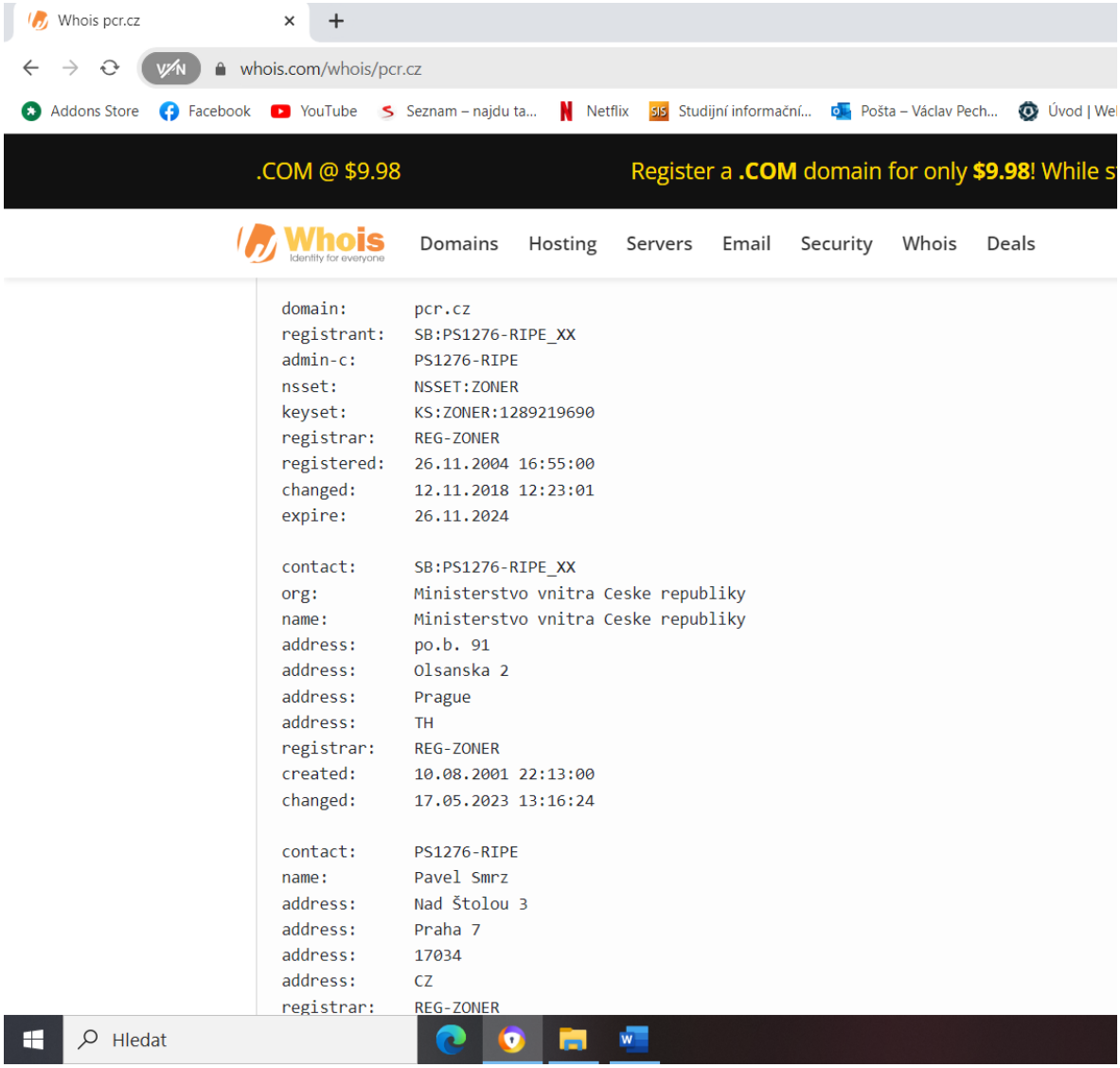


Obrázek 4 – ukázka lustrace IP adresy



Obrázek 5 – ukázka lustrace IP adresy

Na obrázku č. 6 je ukázka lustrace domény pcr.cz se zobrazenými informacemi o registrátorovi.



Obrázek 6 – ukázka lustrace domény

Uvedené internetové stránky jsou možnosti, kde provést ověření při prvotním nebo i následném zpracování případu (existují i jiné). Při prověřování je vhodné použít více internetových stránek (např. kombinaci whois.com a Ipqualityscore.com), zejména z důvodu ověření důvěryhodnosti informace (i když na uvedených internetových stránkách jsou poměrně přesné údaje).

3.2.2 Policejní systémy

Policejní orgán má při prověřování další možnosti, umožňující efektivnější prověřování a vyšetřování kybernetické kriminality, nejpoužívanější jsou tyto informační systémy:

CDO – neboli Centrální databáze objektů – jedná se o databázi umožňující vyhledávání v rámci celé policie (trestné činy, přestupky i čísla jednací, kromě utajených skutků), kde lze vyhledávat dle různých atributů. Už při příjmu oznámení je vhodné prověřit zjištěné atributy, informace, zda se nejedná o sériovou trestnou činnost. Vhodné je to provést dotazem přes „atributy“ a poté dotazem „vyhledávání fulltextem“. Tím při příjmu oznámení může být zjištěno, že případ spadá do nějaké sériové trestné činnosti, kdy tato informace umožní se přizpůsobit konkrétním požadavkům v konkrétním případě (některé informace, úkony nebude nutné udělat, jelikož byly již učiněny, jiné naopak budou mít prioritu; provádí se po konzultaci se zpracovatelem případu do jehož série skutek spadá).

Kriminalisticky sledovaná událost (dále jen IS KSU) je systém jehož úkolem je zjednodušit, zrychlit a zefektivnit využívání informací, které napomáhají policistům při odhalování a vyšetřování trestné činnosti, případně jejímu předcházení, u vyšetřování trestných činů, provinění a některých sledovaných přestupků. Na základě operativních výstupů z IS KSU je možné koordinovat součinnost útvarů. IS KSU také zvyšuje efektivitu v oblasti pátrání po odcizených věcech i pocházející z přestupků. Současně odstraňuje duplicitu některých činností jak na základních útvarech, tak i na analyticko-informačních pracovištích.

IS KSU zavedl nové technologické prvky do analytické činnosti s kriminálními daty, jejichž cílem je mimo jiné zajistit jednotný datový tok do centra, dostupnost pro všechny oprávněné uživatele, okamžitou aktuálnost, ověřenou správnost a kompletnost. Další výhoda je komunikace a vzájemná výměna dat jednak mezi službami uvnitř policie, ale také v rámci zemí EU. V současné době je systém schopen podle stanovených kritérií automaticky vybírat a předávat data do Schengenského informačního systému (dále jen SIS). Prvotní data se do IS KSU získávají z informačního systému, určeného pro základní útvary (IS ZIS 2000,

IS ETŘ) nebo se převádí pomocí klienta pro IS UDÁLOST.

IS Událost – je systém obsahující informace o událostech, případech, spojený s hlášením událostí.[54]

IS telefony – je systém určený ke zpracování osobních údajů účastníků telekomunikačních služeb na základě požadavků policistů PČR, příslušníků SKPV, pro prověřování, předcházení a odhalování trestné činnosti, odhalování pachatelů trestných činů a konání vyšetřování o trestných činech.[55]

AMOS NET KRIM – je mimořádné opatření "NET KRIM", je zaměřeno na potřeby vyhledávání a koordinace typově shodné trestné činnosti spadající do oblasti ostatní trestné činnosti páchané v kyberprostoru, Za účelem zefektivnění objasňování a vyšetřování ostatní trestné činnosti páchané v kyberprostoru.

Vyhledává a zobrazí skryté shody v atributech objektů vedených v lokálních databázích systému ETŘ. Sběr, zpracování a exportování údajů AMOS (dále jen „prostředek AMOS NET KRIM“), umožní koordinované sdílení a vyhodnocování kvalitně zpracovaných informací, a přispěje tak k užší spolupráci mezi útvary a k efektivnějšímu postupu Policie České republiky ve vztahu k vyhledávání a objasňování tohoto typu kriminality.

Jsou zde zpracovávány údaje:

- osob majících vztah ke konkrétnímu, v informačním systému ETŘ evidovanému, případu v postavení prověřovaný, podezřelý, omezený na svobodě, obviněný, hledaný nebo neznámý pachatel (dále jen „zájmová osoba“) v rozsahu jméno a příjmení, datum narození, poslední čtyřčíslí rodného čísla, datum zahájení trestního stíhání a poznámka k osobě, jsou-li známy,

- ve formě kontaktních údajů, které byly k zájmovým osobám zjištěny v rozsahu číslo účtu nebo kryptoměnové peněženky, variabilní symbol (např. v případě sběrného účtu), IBAN, e-mailová adresa, telefonní číslo, IMEI, uživatelské jméno, přezdívka (nick), falešná identita (alias), doména nebo web, identifikátor

[54] Závazný pokyn policejního prezidenta č. 136/2006
[55] Závazný pokyn policejního prezidenta č. 138/2008.

instant messengeru (Skype, ICQ) a VOIP/IP adresa[56].

Oddělení analytiky a kybernetické kriminality (OAKK) – obecným úkolem je odhalování, dokumentování a prošetřování trestné činnosti spojené s použitím informačních a komunikačních technologií. Náplň činnosti se liší podle jednotlivých krajských ředitelství policie. Někde toto oddělení provádí prověřování v rámci celého spisu (sami si vedou spisový materiál) převážně však spisový materiál je na místně a věcně přístupném oddělení (OOP, SKPV) a OAKK provádí zajišťování digitálních stop (komunikace, soubory, bitové kopie, trasování kryptoměn, apod.), šetření k IP adresám, doménám a dalším důkazním prostředkům z kybernetické kriminality. Šetření však provádí mnohdy za užití otevřených zdrojů (jež jsou popsány v předchozí podkapitole), kdy jejich vytížení způsobuje prodlevy u jiných úkonů, které si zpracovatel nemůže zpracovat sám (např. šetření v otevřených zdrojích může udělat zpracovatel, ale na provedení bitové kopie nemá vybavení a proškolení).

Další systémy lze využít pouze prostřednictvím jiných oddělení. Jedná se zejména o:

Útvar zvláštních činností (šetření ke spoofingu, freezing)

Útvar specializovaných činností (provedení předstíraného převodu)

Ředitelství pro mezinárodní policejní spolupráci – umožňuje žádosti, získávání informací z jiných států, zejména v rámci operativního zjišťování informací.

3.3 Rozbor aktuálních případů z praxe

V rámci této diplomové práce jsou popsány aktuální případy z policejní praxe z posledních 2-3 let, které jsou rozděleny do několika kategorií, kdy tyto kategorie tvoří obsáhlejší skupiny jednotlivých případů kybernetické kriminality, jenž jsou si velmi podobné. Pro rozbor je vybrán vždy konkrétní případ, jež je

[56] Zdroj – Úřad služby kriminální policie a vyšetřování policie České republiky, kriminalita páchaná v kyberprostoru

popsán bez uvedení identifikačních dat (jména, příjmení, konkrétní IP adresy apod.) z důvodu ochrany osobních údajů, informací a také z důvodu, že u některých případů stále probíhá prověřování. Uvedené případy jsou evidované na OŘP PRAHA II a ÚO PŘÍBRAM.[57]

Nabídky výhodné půjčky

Případy nabídek výhodné půjčky jsou typické způsobem vedení kontaktu pachatele s poškozeným tak, že poškozený má pocit, že pouze tímto způsobem mu bude umožněno získat půjčku tak výhodnou, jako běžné banky neposkytují.

V takovýchto případech pachatelé po získání důvěry poškozeného jej přesvědčí o zaslání ofocených dokladů (potřebných pro sjednání půjčky), typicky občanský průkaz, řidičský průkaz, povolení k pobytu, výpis z bankovního účtu (na doložení příjmů), případně pracovní smlouvu. Poté požadují po poškozeném zaplatit poplatek (za sjednání, za přeposlání finančních prostředků na bank. Účet apod.). Prostředky si pachatelé nechávají zaslat na jiný bank. Účet (v ČR nebo v cizině) nebo do směnáren s následným převodem do kryptoměn. Cílovou půjčku poškození nedostanou, jsou po nich opakovaně požadovány poplatky s tím, že pachatelé udržují poškozené v tom, že „toto je poslední poplatek, pak Vám přijdou peníze na účet“. Delším kontaktem mezi poškozeným a pachatelem je navýšeno množství digitálních stop (dokumenty, obrázky, zprávy), je vhodné prověřit metadata k nim připojená. Důležité je včasné zajištění dat, jelikož pachatelé poté, co mají podezření, že již od poškozeného nedostanou další peníze, komunikaci mohou smazat (hlavně ve WhatsAppu). Při existenci telefonních čísel lze provést žádosti o zjištění dat telekomunikačního provozu (je dost možné, že půjde o spoofing). Otázka je v případech, kdy byl použit whatsapp jen přes data, zde je možnost užití více zařízení na jedno telefonní číslo (v teoretické rovině by tak pachatel mohl vytvořit falešnou stopu).

Případ půjčky od zahraniční banky (začátek roku 2022)

V tomto případě poškozený hledat výhodnou půjčku pro své podnikání, jíž

[57] Případy jsou popsány na základě osobní zkušenosti autora této diplomové práce, vedl jsem prověřování buď celé nebo jeho část.

by zafinancoval nákup lepšího vybavení pro své podnikání. Na internetu nalezl nabídku na půjčku od zahraniční banky, která nabízela nízký úrok a snadné získání peněz, sjednat ji bylo možné přes internet. Zadal své kontaktní údaje a posléze jej kontaktoval neznámý muž z telefonního čísla ze státu v EU. Muž mluvil s přízvukem (ukrajinským), ale dalo se s ním domluvit. Tento muž poškozenému nabídl výhodnou půjčku, kdy jej odkázal na stránky zahraniční banky, pro níž údajně měl pracovat. Po poškozeném požadoval zaplacení vstupního poplatku na bank. Účet vedený v cizím státě ve střední Evropě (jiný než odkud bylo telefonní číslo. Poškozený pachateli uvěřil a na bank. Účet zaslal aktivační poplatek. Komunikace probíhala přes WhatsApp (z jiného telefonního čísla). Pachatel poté kontaktoval opakovaně poškozeného, po němž požadoval další a další poplatky. Poškozený je platil dle instrukcí, kdy je pachatel požadoval platit pomocí Western Union a WISE. Platby byly odesílány na Ukrajinu, na různá ukrajinská jména. Poškozený takto v průběhu roku a půl z poškozeného na poplatky vyčerpal přes 1,5 milionu Kč. Poškozený sice měl podezření, že se jedná o podvod, ale pachatel jej vždy nějakým způsobem přesvědčil k další spolupráci (zejména tím, že mu ukázal jeho bankovnictví – fiktivní stránky zahraniční banky). Ke konci už poškozený jen doufal, že dostane půjčku, neboť na poplatkách splatil celou jistinu půjčky.

Ve věci byla zajištěna komunikace z WhatsAppu, kde z metadat nebylo zjištěno pozitivních informací, ale byl zjištěn obrázek pasu, kterým se prokazoval pachatel. Dále zde bylo jméno fiktivní osoby (obrázky byly stažené z internetu). Žádostí na WhatsApp nebylo zjištěno pozitivních informací.

K první platbě, která šla na bank. Účet do země ve střední Evropě, kde byl i registrován uvedený pas a jedno z telefonních čísel bylo provedeno šetření přes ŘMPS a posléze vyžádáno EVP, kdy bylo zjištěno, že bank. Účet a tel. Číslo bylo registrováno na jednu osobu, Ukrajince, který však už v zemi není, vrátil se domů na Ukrajinu. Pas byl falešný, žádná taková osoba nebo číslo pasu neexistovalo. V době tohoto zjištění probíhala už na Ukrajině válka s Ruskem, tedy nebylo možné z této země získat odpověď na požadované informace (toho pachatelé poté hodně využívali, používali IP adresy, domény, telefonní čísla registrovaná na Ukrajině nebo v Rusku, kdy k takovýmto informacím nebylo možno získat další

informace). Platby přes WISE a Western Union (firmy mají v česku pobočky, ale sídla mají v jiných zemích) byly vedeny na nějaké osoby na Ukrajině, tedy nebylo možno zjistit, jakým způsobem tam probíhalo ověření osoby, která platby přebírala. Fiktivní stránky byly registrovány v Rusku, k tomuto také nebylo zjištěno více informací. První telefonní číslo bylo typu kreditního tel. Čísla, nebyla zjištěna osoba ani jiná souvislost (ověřováno přes ŘMPS). Případ byl odložen dle § 159a/5 tř.

Zhodnocení případu půjčky od zahraniční banky

Případ byl netypický dlouhým kontaktem mezi pachatelem a poškozeným (přes rok a půl), kdy poškozený opakovaně posílal požadované peníze na údajné poplatky. Pachatelé využili aktuální situace ve světě (válku na Ukrajině) ke ztížení zjišťování dalších informací. Otázka je, zda opravdu došlo k reálným výběrům v dané zemi (byly do lokalit, kde neprobíhaly boje) nebo se jednalo jen o zástěrku, od WISE a Western Union nebyly zjištěny relevantní informace. Dobré důkazní prostředky by byly k osobě, která vlastnila bank. Účet a tel. Číslo, ale osobu nebylo možno zastihnout a vyslechnout, jelikož již zemi opustila (je možné, že se jednalo o organizovanou trestnou činnost, kdy po určité době dochází k výměně osob a tím ztížení vyšetřování). V tomto případu nebyly sice využity zakrývací metody pachatelů, ale i tak se nepodařilo zjistit osobu pachatele. Největším důvodem byla doba uchování dat a nemožnost nebo podstatné ztížení zjištění některých informací.

Nabídka výhodné investice, zúročení vkladu

Případy výhodných investic nebo nabídek s výhodným zúročením vkladu jsou typické kategorií poškozených, primárně se totiž přihodí osobám, které hledají možnosti zúročení svých uspořených peněz. Dost často své kontaktní údaje poškození zadají do nabídky na internetu nebo je přímo osloví osoba vydávající se za bankéře či poradce (pokud poškození nezadali své údaje nikam, pachatelé mohli jejich kontaktní údaje získat jiným způsobem, na darknetu, od jiného pachatele, nabouráním do systému poškozených). Dalším způsobem je kontaktování cizí osobou v návaznosti na komunikaci na Facebooku, Instagramu,

internetové seznamce nebo jiné sociální síti. Zde pachatelé nejdříve získají pár informací o poškozených a poté je přesvědčí o společné investici.

Případ investice do kryptoměn v návaznosti na kontakt na seznamce (z roku 2022)

Poškozená se zaregistrovala na internetové seznamce, kde jí zkontaktoval muž cizí země. Po pár vzájemných textových zprávách muž přesvědčil ženu, že by spolu mohli investovat do kryptoměn. Žena se nechala přesvědčit a poté si stáhla běžně dostupné aplikace k převodu finančních prostředků do kryptoměn. Dle instrukcí pachatele žena během necelého roku poslala na „společné investice“ kolem 7 milionů Kč. Pachatel ženu zmanipuloval s tím, že se setkají v Evropě (muž byl dle jeho vyjádření ze severní Ameriky). Ke kontaktu nikdy nedošlo. Muž sice ženě poslal „své video“, ale reálný kontakt nikdy nebyl. Žena posléze věc oznámila, jelikož kryptosměnárna, kde společně „spořili“ (pachatel tam údajně také posílal peníze), ji zablokovala účet s tím, že je podezření, že se jedná o legalizaci výnosů z trestné činnosti. Komunikace probíhala prostřednictvím Messengeru.

Ve věc byla zajištěna komunikace a provedeno šetření k informacím k osobě pachatele. Video a ostatní údaje byly zřejmě falešné, osoba zobrazena na videu a fotografiích byl herec, který na internetu uvedl, že jeho podobu někdo využil k podvodům. Informace vyžádané k profilu pachatele obsahovali IP adresy typu VPN, vedli také do severní Ameriky, ale z EVP nebyly zjištěny žádné konkrétní informace, reakce byla spíše odmítavá. Od směnárny (sídlo v severní Americe, na jednom z pobřežních ostrovů), která účet měla zablokovat také nebylo zjištěno pozitivních informací, jejich spolupráce nebyla zrovna pozitivní, ale případ se stále prověřuje. Ale pokud nebudou zjištěny v dané věci okolnosti vedoucí k určité osobě či skupině osob, tak bude věc odložena dle § 159a/5 tř.

Zhodnocení případu investice do kryptoměn v návaznosti na kontakt na seznamce

Případ byl překvapivý výší způsobené škody na jedné osobě (poškozená je klasická pracující osoba střední třídy, v průběhu skutku si vzala několik hypoték a

půjček). Zpočátku byla i vyšetřovací verze, že se nejedná o podvod, ale o omyl kryptoměnové společnosti. Ale posléze na základě zjištěných údajů bylo zřejmé, že jedná o promyšlený podvod. Způsob provedení, zejména získání důvěry bylo z časového hlediska zdlouhavé, ale po získání důvěry umožňuje průběžné získávání finančních prostředků z poškozené. Případ se prověřuje již téměř rok, proto je otázka, zda rychlejším a efektivnějším rozpracováním by nebylo získáno více důkazních prostředků (některé už po několika měsících nebyly k dispozici), i když vzhledem k VPN a ostatním okolnostem není jisté, jestli by dané informace vedly k určité osobě.

Případy tradingu

Případy tradingu jsou typické osobami poškozených, kteří hledají možnosti investice, zejména zúročení nákupem kryptoměn. Poškození jsou dvojího druhu – poškození, kteří mají s kryptoměnou zkušenosti (mohou i mít znalosti z této problematiky) a poškození, kteří s kryptoměnou zkušenosti nemají (ty lze snáze přesvědčit, zmanipulovat podle potřeb pachatelů). U pachatelů je výrazná výborná znalost kryptoměn a použití příslušných aplikací (pro převody finančních prostředků, na správu kryptopeněženek).

V poslední době se v tomto objevili nové zajímavé způsoby páchání, popsané v případu níže uvedeném.

Případ tradingu (přelom roku 2023/2024)

Poškozený hledal možnosti zúročení naspořených peněz (kolem 700.000,- Kč), kdy jej zajímala zejména možnost investic do kryptoměn. V dané problematice se orientoval, sledoval vývoj několik posledních měsíců. Na internetu objevil reklamu na možnost investování se zaručeným zúročením zajištěným tím, že umělá inteligence hlídá a předvídá vývoj cen kryptoměn, dochází tak k včasnému převodu finančních prostředků a zefektivnění zisku. Po kliknutí na reklamu byl přesměrován na jinou internetovou stránku, kam zadal své kontaktní údaje. Ozval se (telefonicky, cizí předvolba, komunikace česky, s přízvukem) mu neznámý muž, který mu vysvětlil výhodnost a efektivitu jím nabízených služeb. Prostřednictvím neznámého muže (představil se jako pracovník firmy, která nabízí

investici hlídanou umělou inteligencí) si poškozený nainstaloval běžně dostupné aplikace z google play určených k převodům finančních prostředků (např. ZEN, Atomic Wallet), kam poškozený měl přístup. Pachatel poté přesvědčil poškozeného, aby zaslal první finanční částku, kterou následně převedli společně do peněženky. Poté pachatel ukázal v aplikaci zúročení, zisk, který pak společně poslali na bank. Účet poškozeného. Tímto pachatel zvýšil důvěryhodnost svého jednání, poškozený poté ve spojení s pachatelem zaslal další finanční prostředky (ve výši kolem 700.000,-Kč), které přeposlal do kryptoměny, do peněženky. Do té však umožnil přístup i pachateli, který svůj přístup odůvodnil tím, že v rámci umělé inteligence potřebuje možnost kontroly. Pachatel poškozenému vysvětlil, že v aplikaci (volně stáhnutelné) je nastavené, že umělá inteligence provede automatický převod jeho finančních prostředků do nejvýhodnější kryptoměny, čímž dojde ke zvýšení zisku. Avšak převod finančních prostředků byl proveden do kryptoměny, bez hodnoty (nové kryptoměny vytvořené pachatelem). Tímto ztratili finanční prostředky poškozeného cenu a pachatel je poté přesně nezjištěným způsobem převedl pryč, mimo dispozice poškozeného.

Ve věci byla zajištěna komunikace (přes whatsapp, kde byly zprávy i hovory), byla provedena bitová kopie zařízení a žádosti o informace k jednotlivým aplikacím. Telefonní čísla byla spoofovaná. IP adresy zjištěné od společnosti whatsapp byly typu VPN. Doména na níž byl původní inzerát byla podvodná, registrováno v cizině, více k ní zjištěno nebylo. K údajné firmě více také nebylo zjištěno.

Případ je stále ve fázi prověřování a shromažďování důkazních prostředků, ale pokud nebudou zjištěny skutečnosti vedoucí k určité osobě, bude věc odložena dle § 159a/5 tř.

Zhodnocení případu Případu tradingu

Popsaný případ ukazuje zajímavý způsob páchání kriminality, kdy kontakt mezi pachatelem a poškozeným trvá delší dobu. V rámci získání důvěry pachatel poškozenému zaslal peníze, aby tím získal důvěru. Výrazná je znalost pachatele problematiky kryptoměny.

V uvedeném případu je rozpracované shromáždění a vyhodnocení

informací, kdy z dosavadních informací nebylo zjištěno pozitivních skutečností vedoucích k určité osobě. Možné důkazní prostředky by mohly být zjištěny od společností provozujících aplikace, které byly použité (přístupy, převody), ale otázka je, jakým způsobem budou společnosti komunikovat a jaká konkrétní data budou zjištěna. Ve věci je pravděpodobné, že se bude jednat o sériovou trestnou činnost, jelikož připravenost, malé množství důkazních prostředků i ostatní okolnosti tomu nasvědčují. Pachatel v tomto případě využil možnost vytváření nových kryptoměn, kdy rozdílem v hodnotě kryptoměn byl schopen způsobit škodu poškozenému. Tento způsob vyžaduje větší připravenost a trpělivost pachatele, ale zároveň znesnadňuje odhalení podvodného jednání včas, jelikož pokud poškozeným přijdou nějaké finanční prostředky jako důkaz efektivity investic, je více než pravděpodobné, že odešle poté větší množství finančních prostředků v očekávání většího zisku.

Podvodné zprávy s odkazy na fiktivní internetové bankovnictví

Podvodné zprávy s odkazy do fiktivních internetových bankovnictví mohou přijít emailem, SMS, na Facebooku, do messengeru, WhatsAppu či jiným způsobem. Liší se od sebe způsobem zaslání a odůvodněním, proč je nutné něco někde potvrdit (kliknout na nějaký odkaz). Odkaz však většinou způsobí přesměrování poškozeného na internetové stránky vypadající jako stránky internetového bankovnictví, kde si většinou poškozený může vybrat i svou banku. Tam pak poškození zadají své reálné údaje do internetového bankovnictví, kdy pachatelé obratem údaje od poškozených přepíšou do reálného internetového bankovnictví, čímž získají přístup do bankovního účtu poškozeného. Tam buď rovnou provedou neoprávněné transakce nebo přidají nové zařízení, které označí jako prioritní. Na něj pak chodí potvrzovací SMS a pachatelé tak mají čas na provedení transakcí či zažádání o půjčku či úvěr přes reálné internetové bankovnictví (pachatelé mnohdy využijí přístupu do bankovnictví a rovnou si zažádají o půjčku či úvěr, ten také pak obratem odcizí – dáno možnostmi „předschválených půjček nebo úvěrů“).

Podvodné zprávy můžeme dělit podle modus operandy jednotlivých případů (většinou se jedná o sériovou trestnou činnost):

a) Podvodné zprávy obsahující, popisující výskyt nějakého problému – typické je, že pachatelé ve zprávě předstírají, že se u nějaké společnosti vyskytl problém, jehož řešení je nutné vyřešit přes odkaz ve zprávě (nejčastěji podvodné emaily od firem jako ČEZ, Česká pošta, Netflix, různé banky apod.).
b) Podvodné zprávy na inzertních portálech – většinou pachatel předstírá zájem o nějaké zboží, kdy poškozenému pošle odkaz na „doručovací službu“, která provede předání zboží (používají firmy DPD, Česká pošta či je v odkazu napsána jiná doručovací služba).

V odkazech nemusí být vyžadováno jen přihlášení do internetového bankovnictví, ale může se zde nacházet vyplnění jména příjmení, adresy a čísla kreditní karty. Pomocí čísla kreditní karty jsou pachatelé schopni provést neoprávněné transakce, které provedou přes platební brány nebo kreditní účty bank (to jsou bank. Účty banky, přes něž prochází kreditní transakce, nelze na nich provést jednoznačně zajištění finančních prostředků, jsou to směsné účty), z tohoto důvodu je vhodné při zjištění bank. Účtu české banky v případě možnosti zavolat na infolinku s dotazem, zda se nejedná o bank. Účet kreditního typu, některé banky tuto informaci poskytnou obratem, jelikož se tímto vyhnou vysvětlování, proč nebylo možné zajištění finančních prostředků provést.

Samotné internetové stránky, na něž jsou poškození přesměrování vypadají mnohdy jako reálné stránky internetového bankovnictví konkrétní banky. Tato podoba může být způsobena tím, že pachatelé použijí na vytvoření těchto stránek zdrojový kód reálného bankovnictví. K tomuto kódu se pachatelé mohou dostat několika způsoby, buď jej seženou od zprostředkovatele (na darknetu) nebo jej stáhnou sami (rovnou ze stránek či překonáním zabezpečení banky). Schopnější pachatelé jsou schopni takovýto kód vytvořit sami (jedná se „jen“ o naprogramování internetových stránek k tomu, aby byly schopny provést několik úkonů).

Tyto způsoby kybernetické kriminality je možno odhalit v počátku při podrobném prozkoumání emailových adres a odkazů, obsahují totiž malé rozdíly

oproti reálným emailovým adresám a odkazům dotyčných firem (např. email cez@cez.cz je reálné firmy, ale cez-cez@gmail.com je podvodný nebo odkaz https://bezpecnost.csas.cz je reálný, ale https://bezpecnost-c-s-a-s.com je podvodný). Rozdíly jsou sice nepatrné, ale nechají se na internetu běžně ověřit. Problém nastává, pokud pachatelé pozmění emailovou adresu tak, že není možné ověřit její pravost (např. @pcr.cz, kdy takto jsou zakončený emailové adresy u police ČR) nebo využijí služby firmy nebo programu, jenž je schopen změnit nebo zkrátit URL odkaz (v tomto případě je otázka, jakým způsobem je možno provést změnu URL odkazu, např. „zkracovač URL adresy“, zda je pak možno provést nějaké hodnověrné ověření a předejít tak škodě na majetku).

Při prověřování se vyžadují bankovní informace od jednotlivých bank, kdy jsou často vyhodnocením těchto informací zjištěny přístupy do internetového bankovnictví z IP adres typu VPN z různých zemí po celém světě. Nastává tedy problém se získáním dalších informací. Z emailů jsou pak vyhodnocením zjištěny shodné nebo i jiné IP adresy (opět VPN). Pokud dochází ke kontaktu pře mobilní telefonní čísla, jsou telefonní čísla většinou typu kreditních, kdy k majitelům nejsou další informace. Ovšem některé země mají i tento typ telefonních čísel registrovaný, proto je vhodné si v dané zemi tuto informaci ověřit (např. přes ŘMPS).

V rámci prověřování této kriminality však byl zjištěn problém mající zásadní dopad na prověřování této kriminality. Jedná se o přihlašování do internetového bankovnictví. Bylo nezávisle od několika bank (jejich IT techniků) zjištěno, že **do** jejich **bankovnictví se lze přihlásit i prostřednictvím prohlížečů jako je TOR**, při přihlášení nedochází ke kontrole způsobu přihlášení a jeho případnému omezení. Některé banky se dokonce nebyly schopny k tomuto dotazu vůbec vyjádřit, jejich IT oddělení bylo tímto dotazem „překvapeno“. Tato skutečnost má však významný podíl na zjišťování a zajišťování důkazních prostředků proti pachatelům, jelikož tím, jak je nastaveno zabezpečení u prohlížečů typu TOR, tak není možné tímto způsobem zjistit reálné údaje k pachatelům.

Případ s podvodným odkazem v návaznosti na inzerci zboží na Bazoš.cz (z roku 2022)

Neznámý pachatel pod záminkou zakoupení zboží, vybavení na snowboard v hodnotě kolem 1.500,- Kč, přes aplikaci Bazoš.cz kontaktoval poškozenou, kdy jí následně prostřednictvím aplikace Whatsapp (použil českého mobilního operátora, předplacené tel. Číslo), po domluvení obchodu, nabídl uhrazení částky přes kurýrní službu DPD. Poškozené poté zaslal odkaz, který ale byl fiktivní (což poškozená nevěděla), poškozená na odkaz klikla a byla přesměrována na podvodnou internetovou stránku (registrovanou v cizině), kam zadala své přihlašovací údaje do svého internetového bankovnictví, čímž získal neznámý pachatel přístup do internetového bankovnictví poškozené a provedl v něm neoprávněné transakce, v celkové výši kolem 300.000,-Kč, provedené na české bank. účty. Šetřením bylo zjištěno, že přes bank. Účet poškozené prošli platby v hodnotě několik set tisíc korun českých, které jí byly zaslány z českých bank. Účtů. Šetřením bylo zjištěno, že peníze přišli od dalších poškozených, modus operandy byl podobný. Bank. Účty, na které odešly transakce, byly také dalších poškozených. Kombinováním transakcí pachatel značně ztížil prověřování skutku, jelikož transakcí a použitých bank. Účtů bylo několik, kdy z informací od dalších poškozených nebyly zjištěny skutečnosti, které by vedli k určité osobě. IP adresy byly typu VPN z jiných zemí (země EU). Přičemž časovou prodlevou od spáchání po několika měsících již některá data nebyla k dispozici. K mobilnímu telefonnímu číslu pachatele nebylo zjištěno více, v minulosti (před několika lety) sice jeho telefonní číslo figurovalo v jednom případě, kdy k němu byla osoba, ale tato osoba poté už toto telefonní číslo nepoužívala, telefonní číslo tedy bylo po nějaké době nepoužívání opět zařazeno do prodeje, kdy si jej koupil pachatel, nebylo zjištěno kde a jak. Internetová stránka podvodného bankovnictví byla registrována v cizině, bez dalších informací. Metadata, z nichž by se podařilo zjistit více informací, zjištěna nebyla. Od společnosti WhatsApp bylo zjištěno pár informací, které ale prozatím nevedli k žádné osobě. Pachatel při komunikaci s poškozenými použil několik telefonních čísel a několik IP adres (i falešných internetových bankovnictví), dle poznatků k hlasu pachatele je pravděpodobné, že se jednalo i o několik pachatelů. Ve věci posléze došlo ke spojení s dalšími případy, jedná se o sériovou trestnou činnost, věc je stále prověřována (ale pokud nebudou zjištěny konkrétní okolnosti, věc bude odložena dle § 159a/5 tř.).

Zhodnocení případu s podvodným odkazem v návaznosti na inzerci zboží na Bazoš.cz

Na uvedeném případu je patrné, že pachatelé jsou schopni vytvořit internetové bankovnictví, které vypadá jako reálné. Poškození většinou neprovádí kontrolu odkazu, v danou chvíli nemají podezření na podvodné jednání, jde jim o prodej zboží. Bohužel si poškození většinou ani nekontrolují text autorizující zprávy (tím by nebyla provedena transakce), proto jej také zadají do falešného bankovnictví, tak pachatelé mohou zadat neoprávněné transakce. Tím, že pachatelé v přístupech do bankovnictví používají IP adresy typu VPN, tak je značně ztížena možnost jejich ztotožnění, k tomu navíc je možné, že používají prohlížeče typu TOR, tedy zobrazená IP adresa není reálná IP adresa pachatele. Ve spojením se spoofingem je pravděpodobnost zjištění pachatele značně minimalizována.

Podstatné pro řádné prověření je rychlost vyžádání a zajištění dostupných dat. Možno použít případně freezing dat. V případě transakcí na české účty, tak je nutné zajistit finanční prostředky usnesením (dodržet ale zásadu přiměřenosti a zdrženlivosti).

Případ podvodů na inzertních portálech, prodej zboží (z toku 2022)

V roce 2022 bylo vedeno několik přestupkových podvodů na inzertním portálu bazos.cz, Facebook Marketplace. Postupným sloučením na základě shodných atributů (telefonní číslo, bank. Účet pachatele, alias pachatele) způsobená škoda přesáhla výši 10.000,-Kč. Princip skutku byl takový, že pachatel na inzertních portálech pod různými jmény inzeroval prodej zboží (různého typu, od helem, po motorky, náhradní díly), kdy si za zboží, které měl dodat nechával zaplatit předem, ale zboží nikdy žádné nedodal. Ve věci byly zahájeny úkony trestního řízení a vyžádány informace k jednotlivým bank. Účtům pachatele. Bylo zjištěno, že se jedná o několik osob jejichž výslechy se podařilo zjistit, že svůj bank. Účet zapůjčili svému kamarádovi. K osobě tohoto pachatele následně byly zjištěny další informace (aliasy, telefonní čísla z lustrací, IP adresy) a muž byl následně vyslechnut. K věci se zpočátku odmítal doznat, ale po předložení důkazních

prostředků se k věci doznal. Byl vyzván k vydání věci (svých mobilních telefonů a ostatních zařízení – na nich bylo provedeno znalecké zkoumání). Celková způsobená škoda byla mezi 150.000 – 200.000,-Kč, poškozených je téměř 100 osob. Pachatel inzeroval sice na různých inzertních portálech různé zboží, ale používal stejné fotografie a kontaktní údaje u některých inzerátů. V dané věci bylo také zvažováno po konzultaci se znalcem z oboru informačních technologií, že by se jako důkazní prostředek použili cookies, jelikož při prvním zobrazení internetové stránky dochází k ukládání cookies, které je po určitou časovou dobu jedinečné, lze jej tedy spárovat s určitým zařízením. Skutek je v současné době ve fázi vyšetřování, důkazní prostředky svědčí o vině určité osoby, věc bude skončena návrhem na potrestání osoby a je pravděpodobné, že bude u soudu prokázána vina pachatele.

Zhodnocení případu podvodů na inzertních portálech, prodej zboží

Uvedený případ byl objasněn důkladným shromažďováním a vyhodnocováním důkazních prostředků. Pachatel nepoužíval způsoby překrytí IP adres ani spoofing, jako bank. Účty použil osoby, které jej znají. V souhrnu tyto informace vedli k určité osobě, která se následně k činu doznala. Věc byla objasněna, byť prověřování a shromažďování důkazních prostředků trvalo téměř rok. Doba byla tak dlouhá nejen kvůli množství informací, s nimiž bylo nutno pracovat, ale i tomu, že zpracovatelé měli k tomuto případu dalších téměř 20 jiných případů, na nichž museli pracovat, to v souhrnu způsobuje prodlevy na jednotlivých případech

Zvláštními případy s fiktivními internetovými bankovnictvími jsou případy, kdy jsou napadené internetové stránky, zejména ty, kde nechá platit platební kartou (její digitální verzí). Může se jednat o internetové stránky obchodů, muzeí, divadel, apod. Na těchto internetových stránkách je umožněna platba kartou, kam poškození zadávají číslo své platební karty. Pachatelé zde mohou překonat zabezpečení nebo si jiným způsobem sjednat přístup, kdy zde ponechají škodlivý kód, který jim odesílá data týkající se informací k poškozeným, které poškození zadali (jména, příjmení, adresy, kontakty, číslo platební karty). Pomocí

čísla platební karty jsou poté schopni provést neoprávněné transakce. Teoreticky by je opatrní poškození mohli rozpoznat, v době kdy jim přijde informace o autorizování platby, ale pokud pachatelé změní primární zařízení, poškození se o neoprávněných transakcích dozví až v historii provedených transakcí nebo ve výpisu z bank. Účtu.

V některých případech se nepodaří zjistit jakým způsobem se pachatel dostal do internetového bankovnictví nebo z jakého důvodu byly provedeny neoprávněné platby. Někdy je na vině sám poškozený, jindy je to způsobeno schopnostmi a znalostmi pachatele. Další důvod může být nedostatečné zabezpečení ze strany příslušné banky.

Případ neoprávněných plateb provedených platební kartou po zaplacení na internetu (z roku 2023)

Poškozená si běžným způsobem, jako už několikrát, na internetových stránkách kulturního zařízení objednala lístky, které zaplatila platební kartou. S platbou byl nespecifikovaný problém, kdy platbu zadala 2x. Platba proběhla poté už v pořádku. Autorizace jí přišla na mobilní telefon. Přišlo jí více zpráv, které si ale nepřečetla detailně. Po několika dnech si všimla v bankovnictví, že jí schází několik desítek tisíc korun českých, kdy jí peníze odešli na bank. Účty v jiné zemi, jako transakce platební kartou. Od poškozené bylo zjištěno, že nikam své bankovnictví (kromě uvedené platební karty) nezadávala. Ani si nestahovala nějaký program nebo doplněk. Z výslechu tedy bylo zjištěno, že jediné místo, kam zadávala své údaje bylo na internetové stránky kulturního zařízení. (Nelze ale vyloučit, že by únik údajů poškozené mohl pocházet z minulosti.) Šetřením u technické podpory internetových stránek kulturního zařízení bylo zjištěno, že před několika dny mají v systému zaznamenán nějaký bezpečnostní incident. Je tedy možné, že zde došlo k narušení zabezpečení, ale přesný způsob nebyl zjištěn. Upotřebitelná data zjištěna nebyla.

Platby byly provedeny jako transakce platební kartou, je u nich uvedena pouze doména, přes kterou peníze odešli (zjištěno, že to byl směsný účet pro kreditní transakce, více zjištěno nebylo). Vyhodnocením přístupů do bankovnictví byly zjištěny IP adresy typu VPN u neoprávněných plateb, z jiného státu, bez

dalších informací.

Souvislost s jinými případy zjištěna nebyla. Věc byla odložena dle § 159a/5 tř.

Vyhodnocení případu neoprávněných plateb provedených platební kartou po zaplacení na internetu

Objasněním modus operandy bylo zjištěno, že se pravděpodobně skutek stal tak, jak je popsáno. Dokonce na těchto internetových stránkách poškozená v minulosti bez problému nakupovala. Podezření tedy v daném případě poškozená neměla. Bylo možno se více zaobírat potvrzovacími zprávami, komu byly doručeny v jakém formátu, ale jestliže byly IP adresy typu VPN, informace by pravděpodobně nevedli k určité osobě pachatele. Co se týká narušení bezpečnosti na internetových stránkách, nebylo zjištěno, jakým způsobem tak bylo učiněno, což může být tím, že pachatel po určité době smazal nebo upravil svůj zásah (úpravu, doplněk, který mu zasílal data).

Falešný bankéř, finanční poradce

Případy falešných bankéřů jsou typickým představitelem kybernetické kriminality, s níž se lze setkat na většině policejních oddělení. Pachatelé navazují kontakt s poškozenými, kdy se vydávají za bankéře, finanční poradce, často ve spojení s falešnými policisty, kriminalisty apod. Po získání prvotní důvěry přesvědčí poškozené o tom, aby učinili, co pachatelé potřebují (instalace Anydesku, provedení plateb). Úspěšnost je závislá na manipulativních schopnostech pachatele (na jeho schopnostech sociálního inženýrství). Zpočátku byly převažující případy převodů na jiné bank. Účty, zejména české, ale s tím, jak se rozšířilo používání institutu zajištění finančních prostředků, tak pachatelé začali více převádět finanční prostředky do kryptoměn.

Případ falešného bankéře v kombinaci s falešným policistou (z roku 2022)

Případ byl oznámen seniorkou, jenž vlastnila několik bank. Účtů. Tato žena byla oslovena neznámým pachatelem, který s představil jako pracovník banky (falešný bankéř), volal z telefonního čísla, které se poškozené zobrazovalo jako

telefonní číslo banky (šlo o spoofované telefonní číslo, hovor ve skutečnosti byl proveden přes firmu sídlící v jiném státě, byl to stát v EU). Pachatel poškozené řekl, že její peníze nejsou v bezpečí, v bance se nachází nějaký pracovní, který se chystá její peníze odcizit, proto je nutné její peníze převézt na jiný bank. Účet a to, co nejrychleji. Poškozené se tato skutečnost nezdála, odmítala z počátku spolupracovat, ale jelikož telefonní číslo bylo zobrazeno jako z banky, nakonec si na pokyn pachatele nainstalovala do mobilního zařízení program AnyDesk (umožňujícím připojení na vzdálenou plochu) a přihlásila se do svého internetového bankovnictví. Pachatel v něm následně provedl několik transakcí v celkové hodnotě kolem 2.500.000,-Kč (IP adresy zjištěné byly pouze poškozené). Peníze odeslal na jiný bank. účet u stejné banky (tím docílil rychlého přesunu peněz). Takto seniorce pachatel přeposlal všechny její celoživotní úspory.

V rámci prověřování byla vzhledem k vysokým transakcím (byly ve výši 500.000,-Kč, celková škoda přes 2 miliony Kč) využita možnost a byl zkontaktován kontaktní pracovník z ÚSKPV, ve věci bylo pomocí něj a následně FAÚ zjištěno, že peníze byly poslány na účet, kde však v současné době (transakce byly 1-5 dní staré) již peníze nejsou. Byly vybrány v maximálních částkách na pobočkách (částky 300.000,-Kč, 500.000,-Kč v několika pobočkách v Praze). Peníze byly vybrány majitelkou bank. Účtu, na nějž byly doručeny. Šetřením k majitelce (za přispění FAÚ) se podařilo majitelku ztotožnit (ustanovit) a posléze zkontaktovat. Při zkontaktování byla majitelka podezřívavá, nechtěla, dokonce odmítala spolupracovat. Bylo jí prý řečeno, že se nemá s nikým bavit. Toto jí bylo řečeno jiným policistou, řekl jí totiž, že jí bude volat někdo od policie, ale bude to podvod, od policie dotyčná osoba nebude. Majitelce cílového bank. Účtu se policistou zpracovávajícím tento případ podařilo vysvětlit, že podvodný policista s ní mluvil již před tím, že pravděpodobně byla podvedena a v současné době je nutné ji k dané věci vyslechnout. Majitelka se dostavila a bylo od ní zjištěno, že ji před několika dny oslovil neznámý muž (představil se stejně jako seniorce, jako bankéř) s tím, že její peníze na jejím bank. Účtu nejsou v bezpečí, pracovník její banky se chystá jí odcizit její peníze, kdy si na ní plánuje vzít hypotéku a peníze z hypotéky si ponechat. Majitelka muži nevěřila, na internetu však zjistila, že dle jména takovýto pracovník banky opravdu existuje a číslo, které se jí zobrazovalo bylo

jako telefonní číslo z banky. Přesto však se spoluprací váhala. Kontaktoval jí tedy jiný muž (další neznámý pachatel), který jí uvedl, že je příslušník policie (v hodnosti nadporučík, zařazen na Místním oddělení v Praze), a jenž jí volal z telefonního čísla s předvolbou 974 (předvolbu používá policie), kdy telefonní číslo bylo jako policejní. Na internetu nebylo možné si jméno policisty ověřit, nakonec tedy majitelka účtu podlehla a začala s muži spolupracovat. Falešný policista jí řekl, že spolupracuje s pracovníkem banky (s neznámým falešný bankéř) a prošetřuje zneužití jejích údajů pracovníkem v její bance. Ženu poté kontaktoval opět falešný bankéř, který jí uvedl, že v bance si někdo zneužil její identitu chystá se na ní vzít hypotéku s tím, že už si na ní vzal nějaký úvěr. Falešný bankéř tedy nejdříve přesvědčil ženu, aby vybrala ve velkých částkách peníze ze svého bank. účtu a poté je pomocí bitcoinmatu vložila na bitcoinové peněženky, které jí určil. Důvodnost tohoto převodu vysvětlit tak, že je nutné peníze přeposlat „mimo centrální systém“ (aby se k nim pracovník banky nedostal) s tím, že on je poté vrátí majitelce na „čistý bankovní účet“, který pro ni vytvořil. Žena tedy peníze vybrala (jednalo se o finanční prostředky seniorky) a vložila je do bitcoinmatu v Praze (o tom, co má kam vložit, ji podrobně instruoval falešný bankéř, lze tedy usuzovat, že měl buď místní znalost nebo využil prohlídek na google maps a prohlídek obchodních domů). Když takto učinila, tak jí falešný bankéř sdělil, že aby se zabránilo tomu, aby údajný pracovník banky si na ní vzal hypotéku, musí ona si vzít hypotéku, co jí nabídne banka a tuto vybrat a opět vložit do bitcoinmatu. Falešný bankéř poté peníze jí vrátí na čistý účet a ona peníze vrátí do banky a tím splatí hypotéku, čímž se vyvaruje dluhu u banky. Žena toto tedy učinila a peníze z hypotéky vložila do bitcoinmatu. V průběhu tohoto měla žena pochybnosti od tom, že takto je správné provést, ale opakovaně jí volal falešný policista (ze spoofovaného telefonního čísla), který jí na její žádost zaslal potvrzení o úkonu, jako propustku do práce ženy. Potvrzení o úkonu jí zaslal z emailové adresy končící @pcr.cz, kdy i dokument byl opatřen záhlavím se znakem police ČR a podpisovou doložkou používanou u policie ČR. Složení emailu přes znakem „@“ však bylo složené z jména, příjmení a oddělení, což není klasický způsob složení emailové adresy u policie ČR, tuto skutečnost však žena nemohla v dané chvíli vědět. Odeslala tedy i peníze z hypotéky do bitcoinmatu, kdy jí vznikla škoda

ve výši kolem 1.500.000,-Kč, celkem se seniorkou tedy pachatelé v průběhu přibližně 5 dní způsobili škodu kolem 4.000.000,-Kč.

Samotná majitelka bank. Účtu je podezřelá z trestného činu Legalizace výnosů z trestné činnosti z nedbalosti dle § 217 trestního zákoníku.

Ve věci bylo provedeno trasování kryptoměn a žádost přes ARO (informace vedli k osobě z východní Asie) a šetření u majitele bitcoinmatu (o něj nebyly zjištěny téměř žádné relevantní informace). Trasování vedlo k dalším informacím, které se v současné době prověřují.

Ostatní informace (spoofované telefonní čísla, VPN) k určité osobě nevedli, pokud tedy dalším šetřením nebudou zjištěny informace vedoucí k určité osobě, bude případ odložen dle § 159a/5 tř.

Zhodnocení případu falešného bankéře v kombinaci s falešným policistou

Popsaný případ ukazuje schopnosti pachatelů týkající se týmové spolupráce a jejich technických a znalostních dovedností. Za účelem úspěchu pachatelé vytvořili legendu o tom, že bankovní systém není bezpečný a je potřeba finanční prostředky poslat jinam. Kombinace falešného bankéře a falešného policisty ve spojení se spoofovanými telefonními čísly je pro poškozené velmi těžko odhalitelná. Zejména v kombinaci s tím, že komunikace probíhá i z emailových adres končících @pcr.cz, kdy i dokumenty jsou téměř podobné jako reálné dokumenty policie ČR. Díky rychlému zpracování v kombinaci s využitím FAÚ byla rychle zjištěna další poškozená, ale peníze se již nepodařilo zajistit (rozdíl pár hodin).

Poměrně rychlým zpracováním byly sice zjištěny základní informace v daném skutku, ale vzhledem ke své povaze (spoofing – data jen 14 dní v daném státě, VPN) nevedli k žádné osobě. Trasováním kryptoměn a šetřením byla zjištěna určitá osoba, ale otázka je jakým způsobem tato osoba bude ve skutku zapojena, zda nepůjde o další osobu poškozenou nebo o tzv. „bílého koně“. Vzhledem k tomuto nelze odhadnout, jestli věc bude odložena nebo bude zahájeno trestní stíhání určité osoby.

Vyděračské emaily

Pachatelé s úmyslem finančního obohacení zasílají emaily (nebo i jiné zprávy, ale převážně emaily), v nichž požadují zaplacení finanční částky, kterou si sami určí. Finanční částku ve většině případů požadují zaslat na bitcoinovou peněženku. Důvodnost zaplacení odůvodňují pachatelé tím, že v případě nezaplacení:

a) *zveřejní inkriminující video nebo fotografie* – fotografie, videa, kde je poškozený nahý, onanuje apod. Tyto materiály se pachatelům dostali do dispozice buď:

- z přechozího kontaktu, kdy je z poškozených vylákali, např. vydávávajíce se za osobu mající o poškozeného zájem,
- neoprávněným zásahem, stažením ze zařízení od poškozeného
- nebo je k dispozici pachatelé nemají, ale vyvolají svou výhružnou zprávou dojem, že je mají.

b) *ponechají zašifrovaná data poškozeného či je uveřejní* – může se jednat o data na počítači, notebooku, data soukromé osoby nebo firmy. Tyto data byla pachateli zašifrována neoprávněným zásahem do počítačového systému, kdy pachatelé také mohou zvýšit pocit důvodnosti zaplacení tím, že vyhrožují zveřejněním zašifrovaných dat (na dakrnetu nebo na klasickém inetrnetu.

Email přihází poškozeným z různých emailových adres nebo také může přijít z emailové adresy shodné s emailovou adresou poškozeného (k tomu dojde tak, že pachatel se dostane do emailové schránky poškozeného a odešle email sám sobě nebo v zaslaném emailu přepíše hlavičku zprávy, čímž změní informace přiřazené k emailu).

Podkapitolou výhružných emailů nebo zpráv by mohli být případy týkajících se toho, že pachatel uveřejní inkriminující video nebo fotografii v návaznosti na předchozí kontakt, tedy že pachateli poškozený tyto materiály sám v rámci vzájemné komunikace dobrovolně poslal. Na jednu stranu je to dáno tím, že lidé v současné době hodně komunikují pomocí chatu, seznamek, sociálních sítí. Tím

dochází ke kontaktům s osobami, s nimiž poškození nikdy nebyly v osobním kontaktu, ale zároveň tyto osoby jsou schopny vyvolat v poškozených pocit sounáležitosti nebo výjimečnosti. Tímto způsobem pak pachatelé z poškozených vylákají inkriminující fotografie nebo videa, která posléze použijí pachatelé proti poškozeným s úmyslem získání majetkového profitu s tím, že pokud jim nezaplatí, tak dotyčné materiály zveřejní (na internetové stránky, do časopisu).

Vyděračský email spojený se zašifrováním dat zdravotnické organizace (z roku 2022)

V nejmenované zdravotní organizaci se bez nějakých předchozích náznaků jednoho rána chtěli přihlásit do jejich systému obsahujícího zdravotnické a osobní informace svých pacientů. Při přihlašování zjistili, že data jsou nedostupná, soubory na disku obsahující požadovaná data jsou neznámým způsobem zašifrována, nelze se k nim dostat, použít a otevřít je. V době, kdy převážná část informací k pacientům (jejich diagnóza, způsob léčby, alergie atd.) jsou elektronizovány byla tímto způsobena neschopnost pokračovat v standartním provozu. V podstatě tímto došlo k nepřímému ohrožení i pacientů, jelikož nebylo možno k nim získat jakékoliv informace ze systému. Elektronický systém ukládání dat měl nastaven způsob a frekvenci zálohování, kdy však zálohování způsobilo to, že zašifrovaná data se zkopírovala i na záložní disky, čímž nebylo možno ani ze záložních disků získat data k pacientům. Jediná možnost nějakých informací k pacientům byla z jejich fyzických složek, která sice u některých pacientů byla k dispozici, ale ne v aktuální podobě.

Lékař, který tuto věc řešil si všiml, že soubory mají úplně jinou koncovku, nežli by standartně měli mít. Na počítači se objevila zpráva obsahující informaci, že soubory jsou zašifrovány a pro jejich rozšifrování má napsat zprávu na email (název emailu byl částečně obsažen i ve změně názvu souborů). Ve zprávě po něm bylo požadováno zaplacení finanční částky kolem 18000 amerických dolarů v bitcoinech na bitcoinovou peněženku s tím, že po zaplacení dojde k rozšifrování dat, ale v případě nezaplacení budou data pacientů zpřístupněna na darknetu.

V dané věci bylo provedeno zajištění zašifrovaného serveru (a jeho bitová kopie), jeho odborné zkoumání, kterým ale nebyly zjištěny žádné konkrétní

informace, které by vedly k pachateli.

Prověřením emailové schránky bylo zjištěno, že ve složce odstraněné pošty byl email doručen před několika měsíci, tj. před zašifrováním dat, odeslaný z emailové schránky poškozeného (odesílací i doručovací adresa byla shodná). V emailu psaném anglicky se psalo o tom, že pachatel požaduje zaplatit v bitcoinech, jinak uveřejní inkriminující videa (pachatel inkriminující videa neměl). Na email reagováno nebylo, nikdo si jej nevšiml, ale pachatel zřejmě v této době získal přístup do emailové schránky organizace, kdy tímto získal informace ohledně toho, co organizace dělá a postupně získal přístup k serveru pro následné zašifrování dat.

Prověřením emailů od pachatelů bylo zjištěno, že IP adresy, z nichž byla zpráva odeslána, jsou typu VPN (ze zemí z oblasti Indického oceánu, další informace se k nim nepodařilo zjistit), samotné emaily jsou registrovány u firmy nacházející se sice v EU, ale nemají informace k osobám, na nichž emaily byly registrovány.

Bitcoinová peněženka nebyla použita nepodařilo se jí spojit s žádným případem. V CDO bylo zjištěno, že jedna IP adresa v minulosti byla u podvodu přes internet, ale věc byla odložena dle § 159a/5 tř., jiné spojitosti zjištěny nebyly.

Zda byly údaje pacientů zpřístupněny na darknetu nebylo možné věrohodně ověřit.

Celý případ byl nakonec odložen § 159a/5 tř., jelikož se nepodařilo zjistit žádné informace směřující k určité osobě či skupině osob.

Zhodnocení případu vyděračského emailu spojeném se zašifrováním dat zdravotnické organizace

V prvé řadě bylo důležité objasnit, jakým způsobem došlo k proniknutí do systému. To se podařilo důsledným výslechem lékaře a ohledáním emailové schránky. Původní email však byl starý několik měsíců, tedy data týkající se IP adres již nebyla k dispozici, navíc pachatel použil VPN, tímto způsobem tedy nebylo možno získat více informací. Z nové zprávy bylo zjištěno, že pachatel použil opět VPN, ale z jiné země (a jelikož email byl trochu odlišný, nelze jednoznačně určit, zda se jedná o ten samý případ, i když předpoklad pro to je,

pachatel s postupem času emaily a IP adresy mění). Data z jiné země však stejně k dispozici nebyla, informace byla zjištěna operativní cestou přes ŘMPS. Bitcoinová peněženka byla prověřena v rámci blockchainu, což nevedlo k žádným informacím, nepodařilo se ji spojit s jinými transakcemi, neexistovala. Přicházelo by v úvahu využití předstíraného převodu s následným sledováním transakce, ale problém je v tom, že není zřejmé, že by tento postup opravdu vedl k relevantním informacím, tedy že by napomohl k objasnění činu či dopadení pachatele. Také je problém návratnosti použitých finančních prostředků.

V rámci prověřování byl zajištěn server se zašifrovanými daty. Z něho v teoretické rovině, lze získat informace ke způsobu zašifrování, případně i informace vedoucí k osobě, jenž data zašifrovala. V praxi však zkušený pachatel informace vedoucí k němu za sebou promazává ať sám nebo nastavením smazávání v šifrovacím nebo jiném programu. Zkušený znalec by však teoreticky i z těchto dat mohl získat alespoň nějaká data, která by bylo možno použít, nelze však posoudit, zda v reálu by to u jiného znalce dopadlo se stejným nebo s jiným výsledkem. Problémem u tohoto typu kybernetické kriminality je vysoká znalost pachatelů mnohdy i z oblasti programování, z čehož plyne, že umí efektivně využívat programy a upravovat, mazat informace, které by k nim vedly.

Další problém je, že není úplně možné ověřit na darknetu, zda, kým a kde byly případně informace k pacientům uveřejněny. Je to dáno nejen anonymizovaným způsobem používání darknetu, ale i tím, že u policie není vyloženě možné provést řádné šetření na darknetu a to z důvodu, že to jednak málo osob ovládá a také toho, že jej nelze provádět služebních počítačích (bylo by to extrémně nebezpečné).

Podvodné faktury, žádosti o zaplacení

Případy tohoto typu je možné řadit nejen mezi kybernetickou kriminalitu, ale také ke klasickým podvodům. Smyslem případů je přesvědčení poškozeného o oprávněnosti a správnosti faktury nebo jiného dokumentu zakládajícím povinnost finančního plnění. Vytvoření falešné faktury není v dnešní době nic obtížného, lze jej provést i na běžném počítači, nejsou potřeba žádné speciální nástroje či programy. V některých případech to může být složitější, zejména pokud je

předmět zakládající povinnost finančního plnění specifický, či má nějaké specifické prvky nebo doplňky (např. elektronické podpisy nebo jiné způsoby elektronického či jiného ověření pravosti).

Z popsaného případu vyvstává důležitá otázka a to, jestli mnohé z podobných případů nejsou skryty v latentní kriminalitě (zejména v případech, kdy dochází k postupnému předkládání podvodných faktur, čímž nedojde k odhalení protiprávní činnosti).

Podvodná faktura spojená s napadením emailového systému (z roku 2022)

Česká firma sídlící v Praze zabývající se marketingem, jejíž služby využívají i firmy z jiných států, obdržela žádost o proplacení faktury na přibližně 2 miliony Kč. Tato faktura byla doručena účetní této firmy emailem z emailové adresy její kolegyně, s níž byla zvyklá řešit proplácení faktur pro různé firmy. Ve standartním případě na základě jejího požadavku zaslaného emailem účetní následně provedla zaplacení požadované faktury, jednalo se o faktury, kdy proplacení spěchalo. U této faktury však účetní na ranní poradě kolegyni konfrontovala s tím, že to je už 2 faktura za poměrně vysokou částku, kterou po ní chtěla uhradit. Kolegyně však vyjádřila nesouhlas s tím, že žádnou fakturu jí neposílala. Kontrolou emailu bylo zjištěno, že z emailové adresy kolegyně, byl zaslán email s přiloženou fakturou na 2 miliony Kč z předešlého dne. Navíc však bylo zjištěno, že na číslo bankovního účtu napsaného ve faktuře (registrovaném u banky ve státě EU), byla před 2 týdny zaslána platba ve výši kolem 1 milionu Kč, kdy faktura k tomuto proplacení byla také poslaná z emailové adresy kolegyně. Oba emaily byly psány způsobem, jaký byl obvyklý v komunikaci mezi účetní a kolegyní. Dalším prověřením podivných faktur firma zjistila, že s firmou uvedenou na faktuře nemá aktuální smlouvu, tedy důvodnost fakturace není jednoznačně oprávněná. Avšak první faktura na 1 milion Kč byla proplacena. Důvodem toho, proč účetní fakturu proplatila bylo, že ji přišla od její kolegyně, s níž občas takto řešila proplacení některých faktur, nebyl to tedy ojedinělý případ. Email navíc byl psán téměř shodným způsobem, kterým s ní komunikovala její kolegyně. Účetní tedy neměla podezření, že by se jednalo o podvodnou fakturu. Škoda vznikla firmě ve výši kolem 1 milionu Kč na základě proplacení jedné podvodné faktury.

Ve věci byly zajištěny emaily, které obsahovali podvodné faktury. Emaily byly odeslány z emailové schránky kolegyně, která komunikovala s účetní. Podvodné emaily však nebyly v odeslaných zprávách, ale byly v koši, připravené ke smazání. IP adresy uvedené v hlavičce byly typu VPN z Asie, nepodařilo se k nim zjistit další informace. Metadata z faktur také neobsahovala žádné relevantní informace. Šetřením u firmy se podařilo zjistit, že neznámým způsobem došlo k narušení zabezpečení emailové komunikace, pravděpodobně stažením nebo zobrazením nějakého souboru obsahujícím neznámý škodlivý kód.

V rámci údajů z faktury bylo provedeno EVP do země, kam směřovala transakce z podvodné faktury. Ve stejné zemi (střední Evropa) bylo uvedeno, že je i sídlo firmy (bank. Účet byl na firmu). EVP bylo tedy směřováno ke zjištění majitele bank. Účtu, jeho výslechu a zjištění a výslechu jednatele firmy. Výsledkem (po téměř půl roce od vyžádání EVP) bylo zjištěno, že osoba majitele bank. Účtu a jednatele firmy je stejná osoba. Ale tato osoba byl místní „bezdomovec“ (osoba bez trvalého domova, alkoholik, nalezena na základě místní znalosti policejních orgánů), který neměl žádné počítačové či jiné specifické znalosti, byl před několika měsíci, téměř rokem, osloven neznámým mužem, kterého viděl jen jednou v životě, jenž mu nabídl finanční odměnu za to, že půjde do banky, založí si bank. Účet, od něhož přístupové údaje předá neznámému muži. Další finanční odměnu „bezdomovec“ obdržel za to, že na příslušném úřadě zřídil novou firmu na své jméno, dle instrukcí neznámého muže, kterému pak předal veškerou dokumentaci. Faktickým uživatelem bank. Účtu a firmy byl tedy neznámý muž, kterého se ale nepodařilo blíže již dohledat (obecný popis bez specifických znaků).

V rámci ČR nebylo dle atributů zjištěno, že by byl evidován podobný případ. Věc byla odložena dle § 159a/5 tř.

Zhodnocení případu Podvodné faktury spojené s napadením emailového systému

V prvé řadě je u tohoto případu zajímavá skutečnost, že pokud by od pachatele nepřišla druhá podvodná faktura v relativně krátkém časovém období, bylo by proplacení první faktury přehlédnuto. Je to sice podmíněno i vysokým ročním obratem firmy, ale pokud by pachatel druhou fakturu poslal až za několik

měsíců na podobnou částku (a ne dvojnásobek), je možné, že případ by nebyl vůbec zaznamenán. V návaznosti na tento případ však došlo, nejen u této firmy, ke změně způsobu ověřování a proplácení faktur.

Dalším zajímavým faktorem je to, že pachatel poté, co získal přístup do emailové komunikace firmy, zjistil, jakým způsobem a kdo s kým komunikuje. To mu umožnilo vydávat se za konkrétní osobu zaměstnance firmy a poslat tak podvodnou fakturu účetní. Tato skutečnost ukazuje na schopnosti pachatele analyzovat zjištěné skutečnosti a naplánovat další postup.

Správným krokem bylo zajištění emailové komunikace. Jejím vyhodnocením bylo zjištěno použití IP adres typu VPN z Asie (stejně jako v tomto případu, tak se obecně z Asie většinou nepodaří včas zjistit další konkrétní informace). Tato skutečnost ve spojení s informacemi od IT techniků z firmy vylučovala možnost, že by v dané věci byl zapojen nějaký zaměstnanec (byť tato možnost nebyla v rámci vyšetřovacích verzí zcela vyloučena, ale jelikož se nepodařilo zjistit žádné důkazní prostředky, které by ji podpořili, nebylo možno ji rozpracovat).

Jelikož finanční transakce byla směřována na bank. Účet, vedený na firmu bylo vyžádáno EVP z dané země. Z EVP tedy bylo zjištěno, že pachatel využil jinou osobu k založení bank. Účtu a firmy. Pachatele se tedy nepodařilo dohledat. V době zjištění těchto informací již nejsou k dispozici žádné kamerové záznamy, či jiné informace kromě paměťových stop, protože komunikace mezi „bezdomovcem“ a pachatelem byla přímá bez použití telekomunikačních technologií.

Vzhledem ke způsobu spáchání činu je možné, že pachatel tímto způsobem podvedl vícero firem, kam zaslal podvodnou fakturu. V rámci ČR sice nebyla zjištěna shoda s jiným případem, ale v rámci EU by tato možnost by dost možná, prověření této možnosti by v daném případě mohlo pomoci se zjištěním dalších informací. Otázkou zůstává, jestli by shromážděné informace vedli k určité osobě.

4 Možnosti zvýšení efektivity objasňování kybernetické kriminality

Jak je patrné z kapitoly 3.3 Rozbor aktuálních případů z praxe a tabulek č. 2-4 v podkapitole 2.2.1, úspěšnost odhalování kybernetické kriminality příliš vysoká veliká (např. oproti násilné kriminalitě, kde je objasněnost v rozmezí 50-65 %). Problém s odhalováním a zejména s dokazováním viny pachatelů tkví hlavně v možnostech překrývání, změn či smazání informací, digitálních stop, které by mohli vést k určité osobě. Zejména u inteligentních a organizovaných pachatelů je objasněnost nízká. Situace s možnostmi získání relevantních informací, jež lze použít jako důkazní prostředky, se postupně zlepšuje zejména v oblasti mezinárodních spoluprací, problém je ale časový faktor mezi vyžádáním a získáním informací. Sice se v rámci spolupráce zřizují a využívají společné vyšetřovací týmy, které umožňují efektivnější spolupráci, ale množství činů, které se prověřují tímto způsobem je minimální, většina případů je odkázána na klasický postup (tedy vyžadování informací, šetření přes ŘMPS, ARO).

Pro zvýšení efektivity s ohledem na možnosti zastírání a změn informací o pachateli přichází v úvahu zejména 2 možnosti:

- **Předstíraný převod** – jenž v současné době již lze realizovat prostřednictvím ÚSČ a poté nechat trasovat pomocí ÚZČ. Problém je však návratnosti užitých finančních prostředků, s čímž je spojena schopnost reálně použité finanční prostředky sledovat (trasovat), aby nedošlo k tomu, že je pachatel přesměruje takovým způsobem, že dojde k jejich ztracení. Bohužel s ohledem na negativa se tato možnost zatím příliš nevyužívá.
- **Vytvoření sledovacího algoritmu** – stejně jako jsou pachatelé schopni získávat data od poškozených, je možné vytvořit podobný škodlivý kód (malware, trojského koně), který se odešle pachateli (např. v souboru obsahujícím potvrzení o platbě či fotografii), kdy po zobrazení (otevření) tohoto souboru dojde k odeslání dat na určené místo, do určeného zařízení. Data, která by takto byla odeslána by byla zejména informace o zařízení, poloha, aktuální IP adresa apod. Tím, že by došlo k odeslání

informací v reálném čase, bylo by teoreticky možné obejít možnosti změn dat, jež pachatelé využívají. Tato možnost by v teoretické rovině byla možná použít s odkazem na Sledování osob a věcí (§ 158d tř.), ale reálně v současné době není toto řešení nejvhodnější (zásada přiměřenosti a zdrženlivosti), právní řád tedy neumožňuje plnohodnotné použití tohoto prostředku. Nicméně některé organizace (z USA) tuto metodu v minulosti již použily, kdy na základě shromážděných dat byly schopni rozkrýt celou organizovanou skupinu pachatelů. Tato možnost se v současné době částečně zkouší (zejména jaké jsou možnosti získání informací, problém je s případným antivirovým programem pachatele, odhalení škodlivého kódu, apod.).

Kapitolou samu pro sebe, která by mohla vést k efektivnějšímu zpravování a objasňovaní kybernetické kriminality je kvalita zpracování a rozsah příslušných právních norem. V současné době sice dochází ke změně příslušných zákonů, ale jedná se spíše o reakci na stávající stav. Sice se do nich už promítá odhad budoucího vývoje, ale realita teprve ukáže, jaký dopad na samotnou kybernetickou bezpečnost a prověřování a vyšetřování kybernetické kriminality novelizované nebo nové právní předpisy budou mít.

5 Závěr

Kybernetická kriminalita se stala postupně nedílnou součástí celkové kriminality, a tedy i častou praxí orgánů činných v trestním řízení. Z počátečního „tápání“ v novém a složitém prostředí informačních a komunikačních technologií bylo vytvořeno několik metodik a doporučení na prověřování a vyšetřování kybernetické kriminality. Problém však tkví ve stále nových a mnohdy složitějších způsobech páchání této trestné činnosti, přičemž možnosti překrývání, změn či mazání digitálních stop pachatelů se výrazným způsobem podepisují na nízké objasněnosti této trestné činnosti. Další věcí, která může snížit pravděpodobnost na řádné objasnění a prokázání viny pachatele jsou chyby při zpracování této kriminality. Cílem této diplomové práce, jenž se v rámci možností podařilo splnit, bylo vytvoření uceleného dokumentu, jenž by poskytl informace z oblasti teorie (vysvětlení pojmů) i praxe (úkony souvisejících se zpracováním) a umožnil tak alespoň o trochu efektivnější zpracování kybernetické kriminality.

V teoretické části jsou popsány nejdůležitější pojmy a instituce, v nichž je potřeba se orientovat. Ve statistických datech je patrný nárůst skutků a nízká objasněnost. Ve statistice kriminality od Policie ČR je zajímavý rozdíl mezi prosincem a lednem následujícího roku (z CDO patrný není), kdy tento rozdíl může mít několik důvodů:

- Oznámení činu je rozloženo do jiného časového období
- Došlo reálně ke snížení této trestné činnosti
- Došlo ke změně ve vykazování (možno i na základě novelizace zákonů nebo usměrnění činnosti).

V praktické části byl vytvořen základní rámec úkonů při příjmu oznámení i základního následného prověřování s uvedenými možnostmi prověřování a získávání dalších informací. Z rozboru jednotlivých případů kybernetické kriminality je patrná nízká objasněnost v závislosti na nízkém množství důkazních prostředků vedoucích k určité osobě či skupině osob. Možnosti ke

zvýšení efektivity by mohly poskytnout šanci na zvýšení objasněnosti, ale jejich reálné využití je prozatím sporadické.

Pro zkvalitnění prvotního zpracování byla zpracována příručka pro policisty obsahující základní informace – v samostatném souboru.

Predikce vývoje kybernetické kriminality počítá spíše s rozvojem této trestné činnosti, kdy do této problematiky bude spadat stále více trestných činů. Rozvoj bude i ve způsobech páchání, přičemž s ohledem na vynalézavost a schopnosti pachatelů je otázka, jakým způsobem se bude dařit objasňovat tuto trestnou činnost. To bude závislé nejen na schopnostech člověka (pachatele, vyšetřovatele, obětí) ale i na možnostech plynoucích z prostředí, v němž se daný člověk bude vyskytovat. Pachatel s dobrým zázemím a kvalitním vybavením bude mít vždy výraznou výhodu oproti ostatním osobám (vybavení u justičních orgánů je sice postupně obměňované, ale jeho výkon a rychlost obměn je závislé na rozpočtu a dalších k tomu připojených faktorech). Oproti tomu dobře nastavené právní normy a snížené možnosti překrývání či změn digitálních stop, mohou justičním orgánům zajistit včasné a efektivní zajištění důkazních prostředků, na základě nichž by bylo možné zahájit trestní stíhání daného pachatele (nebo skupiny pachatelů).

Obecně ale lze říci, že orgány činné v trestním řízení budou vždy ne o krok, ale několik kroků pozadu za pachateli. Nezbývá tedy nežli **prověřování a vyšetřování kybernetické kriminality vést důsledně, rychle a efektivně. Pro zpracovatele je důležité se nebránit učení novým věcem a rozvíjet své schopnosti, znalosti a dovednosti.**

Seznam použité literatury

Učebnice a odborné publikace

BANDLER, John a Antonia MERZON. CRC Press/Routledge/Taylor & Francis Group, 2020. ISBN 9780367196233.

BIELSKA, Aleksandra. *Open Source Intelligence Tools and Resources Handbook.* I-INTELLIGENCE, 2020. [online]. [10. 6. 2022]. Dostupné z: https://documentsn.com/document/158a_open-source-intelligence-tools-and-sources-handbook.html.

KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC ISBN 978-80-88168-15-7.

Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech, kolektiv autorů, Praha 2020

MUSIL, J., KONRÁD, Z., SUCHÁNEK, J. *Kriminalistika*, 2. přepracované a doplněné vyd., Praha, C.H.Beck, 2004

PAPÍK, Richard. *Strategie vyhledávání informací a elektronické informační zdroje*. 1. vyd. Praha: Velryba, 2011. ISBN 978-80-85860-22-1.

Radim POLČÁK, František PÚRY, Jakub HARAŠTA a kol. Elektronické důkazy v trestním řízení ISBN 978-80-210-8073-7

STRAUS, Jiří Straus, PORADA, Viktor a kol. *Teorie, metody a metodologie kriminalistiky.* Plzeň, 2017

Trestněprávní ochrana před kybernetickou kriminalitou, JUDr. Kolouch, JUDr. Volevecký, Praha 2013

VONDRÁČEK, Ondřej. *Příručka pro rozkrývání vlastnických struktur a skutečných majitelů.* Transparency International – Česká republika, 2017. Dostupné na WWW: https://www.transparency.cz/wp-content/uploads/Příručka-pro-rozkrývání-vlastnických-struktur-a-skutečných-majitelů-ČJ.pdf.

Vědecké články

PhDr. Marek Hejduk, MBA Policejní akademie České republiky v Praze Bezpečnostní teorie a praxe 1/2021 vědecký článek

Závazné pokyny policejního prezidenta

Závazný pokyn policejního prezidenta č. 103/2013

Závazný pokyn policejního prezidenta č. 136/2006

Závazný pokyn policejního prezidenta č. 138/2008

Internetové zdroje

https://www.atcmarket.cz – web zabývající se prodejem produktů z oblasti výpočetní techniky a telekomunikací.

https://www.czechwealth.cz – web zabývající se burzou a s ní spojenými informacemi.

https://www.internetembezpecne.cz – web zabývající se osvětou kybernetické bezpečnosti

https://www.mioweb.cz - mioweb se zabývá digitalizací podnikání, vysvětlením jednotlivých možností a nabídkou.

https://www.policie.cz – webové stránky Policie ČR

https://www.sprava-site.eu/ - je uskupení osob, které se zabývají správou sítí, podporou a provozem informačních systémů.

Intranetové zdroje PČR

Intranetové stránky Úřadu služby kriminální policie a vyšetřování

Intranetové stránky Národní centrály proti terorismu, extremismu a kybernetické kriminalitě SKPV