Michaela Jurisová

Vybrané kriminologické aspekty podvodov páchaných prostredníctvom falošných manažérov

Anotácia: Cieľom predmetného príspevku je poukázanie na takzvané CEO (z angl. Chief Executive Officer – trestné činy podvodu páchané prostredníctvom pokynu takzvaného „falošného manažéra“)[1], podvody, ako relatívne novú a závažnú formu kriminality. Z analýzy hlásení o neobvyklých obchodných operáciách vyplynulo, že medzi najčastejšie prípady legalizácie príjmov z trestnej činnosti a ich naviazaniu na predikatívnu trestnú činnosť v roku 2018 patrili (okrem iných) aj CEO podvody, čo je jedným z dôvodov venovania pozornosti tejto téme. Na predmetnú kriminalitu je nazerané optikou kriminológie. V teoretickej časti príspevku je poukázané na trestno-právny rozmer, fenomenológiu, páchateľov a ich modus operandi, objekty takýchto podvodov či možnú prevenciu. Teoretická časť príspevku je doplnená o poukázanie na reálne prípady z aplikačnej praxe v podobe kazuistík. K sumarizácii informácií boli využité predovšetkým poznatky finančnej spravodajskej jednotky a úradu kriminálnej polície, tiež odborná literatúra a právne dokumenty. Z metodologického hľadiska boli prioritne využitými: štúdium odborných dokumentov a kazuistiky.

Kľúčové slová: podvod, CEO podvod, legalizácia príjmov z trestnej činnosti, neobvyklá obchodná operácia, Úrad kriminálnej polície Prezídia Policajného zboru, Finančná spravodajská jednotka národnej kriminálnej agentúry Prezídia Policajného zboru, Slovenská republika.

Úvod

Závažné organizované podvody je možné považovať za jeden z vývojových trendov a sprievodných znakov kriminality. Je na mieste uplatňovanie kontroly kriminality, tak v podobe prevencie ako aj represie, z národného ako aj medzinárodného uhla pohľadu. V roku 2014 v rámci Europolu, z iniciatívy Francúzskej republiky, bola zahájená procedúra k otvoreniu nového takzvaného FP (z angl. Focal point[2]) zameraného na závažné organizované podvody. Dôvodom bolo, že Francúzska republika aj ostatné členské štáty Európskej únie zaznamenali počas posledných rokov zvýšený počet takzvaných CEO podvodov (trestný čin podvodu spáchaný prostredníctvom pokynu falošného manažéra, z angl. **C**hief **E**xecutive **O**fficer). Následne v roku 2015 bol zriadený FP APATE (z angl. Focal point Apate[3]), do ktorého sa Slovenská republika zapojila prostredníctvom NAKA P PZ (ďalej aj „Národná kriminálna agentúra Prezídia Policajného zboru). V tejto skupine sú prioritne participujúcimi štátmi Francúzska republika, Španielske kráľovstvo, Belgické kráľovstvo a Rumunsko, pričom je otvorený aj pre ostatné štáty Európskej únie.

Vyplývajúc zo závažnosti predmetnej problematiky, tak ako bolo vyššie naznačené, venuje Úrad kriminálnej polície Prezídia Policajného zboru (ďalej aj „ÚKP P PZ) pozornosť aj CEO podvodom, a to v podobe spracovania správy o vývoji trestnej činnosti CEO podvodov na území Slovenskej republiky (vyplývajúc zo správ jednotlivých odborov kriminálnej polície okresných a krajských riaditeľstiev Policajného zboru) aj analýzy trestnej činnosti CEO podvodov v Slovenskej republike. Predmetnej problematike venuje pozornosť aj finančná spravodajská jednotka národnej kriminálnej agentúry Prezídia Policajného zboru. Aktuálne poznatky (okrem iných) k CEO podvodom je možné nájsť aj vo výročnej správe finančnej spravodajskej jednotky za rok 2018. Dokumenty analyzujú aktuálny stav týchto podvodov, vývoj tejto trestnej činnosti či navrhujú opatrenia de lege ferenda.

---

[1] Pozn. autorky: bližšie k CEO podvodom pozri v texte príspevku.

[2] Pozn. autorky: „špecifická skupina analytického pracovného súboru“.
Bližšie pozri: Správa o vývoji trestnej činnosti CEO podvodov na území Slovenskej republiky.

[3] Pozn. autorky: Apate je jeden z projektov Europolu (Analysis Projects) – kladie osobitný dôraz na boj proti CEO podvodom, ale tiež aj iným podvodom.
Europol.europa.eu. [online]. [cit. 11.06.2019]. Dostupné na internete: <https://www.europol.europa.eu/crime-areas-trends/europol-analysis-projects>.

V texte predmetného príspevku je venovaná pozornosť vybraným kriminologickým aspektom CEO podvodov, vzhľadom na fakt, že na túto trestnú činnosť možno nahliadať multidisciplinárne.[4]

Vybrané kriminologické aspekty CEO podvodov

CEO podvod je cielený útok, ktorého pointou je oklamanie zamestnanca, zvyčajne z finančného alebo účtovníckeho oddelenia. Pri realizácii podvodov je vyvíjaný tlak na zamestnanca spoločnosti aby previedol značné sumy peňazí (do zahraničia). Uvedené podvody sú spájané s takzvaným sociálnym inžinierstvom. Podvodníci pritom využívajú klasické triky sociálneho inžinierstva, prostredníctvom ktorého cez verejne dostupné internetové stránky, ale aj prostredníctvom „nabúrania sa" do e-mailovej komunikácie príslušnej spoločnosti, zistia údaje o prebiehajúcich obchodoch, kontaktoch, spôsoboch komunikácie a samotnej identite CEO manažéra či zodpovedného zamestnanca za prevody peňazí. Páchatelia následne vydávajúc sa za CEO manažéra (zvyčajne e-mailom alebo telefonicky, navodiac atmosféru časovej tiesne), kontaktujú príslušného zamestnanca z dôvodu potreby uskutočnenia finančnej transakcie. V rámci takejto komunikácie nedajú „svojmu podriadenému" na výber a táto je vedená formou striktných pokynov (často aj v spojitosti s hrozbou sankcie za nesplnenie pokynu). Po prevode peniaze končia v inom štáte, kde sa ďalej „prepierajú".

Ide o pomerne novú formu kriminality. Takýto druh podvodu začal byť diskutovaný v rokoch 2007 – 2008. Prvotne bol zameraný prioritne na francúzske spoločnosti. Neskôr, približne v roku 2013, boli takéto prípady zaznamenané aj v ďalších, iných krajinách, ako napríklad Veľká Británia, Belgické kráľovstvo či Rumunsko. Francúzsko ale bolo a aj súčasne je stále miestom s výskytom najväčšieho počtu poškodených/obetí.

Pri CEO podvodoch ide v podstate o „podvod s platobným príkazom". Je charakterizovaný sofistikovaným, zosúladeným a vypočítavým útokom, najmä voči spoločnostiam, ale aj súkromným osobám či štátnym inštitúciám. Útoky sú zväčša organizované jedinou riadiacou skupinou. Základný model podvodu zahŕňa minimálne dva štáty (často členské štáty Európskej únie).

Veľmi podstatným znakom CEO podvodov je konanie, ktoré zároveň tento druh trestnej činnosti posúva do sféry takzvaných „cyber zločinov". Samotný prehľad o vytipovaných spoločnostiach nie je postačujúci. V zásade na vytvorenie dojmu konania oprávneného CEO manažéra je podstatným krokom prelomenie zabezpečenia e-mailovej komunikácie samotného CEO manažéra, za predpokladu, že jeho schránka obsahuje informácie o prebiehajúcich obchodných aktivitách, ale aj o e-mailových adresách jednotlivých zamestnancov. Ruka v ruke s dnešnou dobou sú čoraz častejšie využívané vysoko sofistikované nové technológie zabezpečujúce anonymitu páchateľov.

Táto forma podvodu sa ukázala a stále aj ukazuje ako veľmi lukratívny príjem organizovaných skupín. Vzhľadom na tento fakt, je na mieste CEO podvodom venovať pozornosť z viacerých, rôznych uhlov pohľadu.[5]

V zmysle *trestno-právneho rozmeru* sú zaznamenané prípady CEO podvodov v Slovenskej republike kvalifikované ako trestný čin podvodu podľa § 221 Trestného zákona (ďalej aj „TZ")[6]. V závislosti od spôsobu spáchania, respektíve škody potom prichádza do úvahy kvalifikovaná skutková podstata tohto trestného činu.

---

[4] Bližšie pozri: Správa o vývoji trestnej činnosti CEO podvodov na území Slovenskej republiky.

[5] Bližšie pozri: Analýza trestnej činnosti CEO podvodov v Slovenskej republike.

[6] V zmysle Zákona č. 300/2005 Z. z. TZ - § 221 Podvod

(1) Kto na škodu cudzieho majetku seba alebo iného obohatí tým, že uvedie niekoho do omylu alebo využije niečí omyl, a spôsobí tak na cudzom majetku malú škodu, potrestá sa odňatím slobody až na dva roky.

Ako už bolo aj vyššie uvedené, pri týchto prípadoch môže prichádzať do úvahy aj súbeh trestného činu podvodu (podľa § 221 TZ) a *trestných činov počítačovej kriminality* podľa § 247 TZ a nasl. alebo tiež aj *trestného činu legalizácie príjmov z trestnej činnosti* podľa § 233 TZ.[7]

Z pohľadu *fenomenológie* je na mieste upriamiť pozornosť na pozitívnu zmenu v zmysle doplnenia kódu 858 v číselníku č. 2 Evidenčno-štatistického systému kriminality (ďalej aj „EŠSK“) – Podvod v súvislosti s falošným prevodom peňazí na základe pokynu fiktívneho manažéra. Účinnosť predmetnej zmeny je od 1. októbra 2017 a jej zmyslom je štatistické sledovanie CEO podvodov. Jedným dychom je na mieste dodať, že spätným preverovaním týchto údajov bolo zistené, že prípady vykázané v tejto položke boli/sú vypĺňané nekorektne, pravdepodobne z dôvodu zlyhania ľudského faktora.

V zmysle informácií z jednotlivých krajských riaditeľstiev Policajného zboru (ďalej aj „KR PZ“) bolo v roku 2018 zaznamenaných 27 prípadov CEO podvodov. Z toho bolo pätnásť prípadov spáchaných v štádiu pokusu a v dvanástich prípadoch išlo o dokonaný čin. V roku 2018, v porovnaní s rokom 2017, CEO podvody v Slovenskej republike vykazujú klesajúcu tendenciu. V zmysle trendu vývoja, v roku 2018 bolo zaznamenaných o 18 prípadov menej ako v roku 2017. Na základe dostupných informácií (od roku 2013) je možné konštatovať, že v rokoch 2013 až 2016 zistené CEO podvody vykazovali stagnujúcu tendenciu (do 20 prípadov ročne). V roku 2017 bola zaznamenaná stúpajúca tendencia, na viac ako dvojnásobok v porovnaní s predchádzajúcimi rokmi a v roku 2018 bola opäť zaznamenaná klesajúca tendencia. Teda z dlhodobejšieho hľadiska možno pozorovať stagnujúcu alebo klesajúcu tendenciu zaznamenaných CEO podvodov, s výnimkou v roku 2017. V sledovanom období (v rokoch 2013-2018) vykazovali počty pokusov vyššiu hodnotu ako počty dokonaných skutkov. Z pohľadu kriminálnej geografie bol v ostatnom roku najvyšší počet zistených CEO podvodov zaznamenaný opäť (tak ako aj v roku 2017) v Bratislavskom kraji a najnižší v Prešovskom kraji.

K fenomenologickému poňatiu nepochybne patrí poukázanie na objasnenosť (vybraného činu/druhu kriminality). V prípade CEO podvodov, rovnako ako v predchádzajúcom období, sa ani v roku 2018 nepodarilo objasniť ani jeden prípad. Úroveň objasnenosti uvedenej trestnej činnosti je obmedzená skutočnosťou, že ide o medzinárodnú trestnú činnosť (a prítomnosť prvkov ako „money mule“[8] či zahraničné bankové účty, na ktoré sú prevádzané podvodne vylákané finančné prostriedky). V prípadoch prerušenia trestného stíhania sa ukazuje ako hlavný dôvod nezistenie konkrétnej osoby páchateľa, ktorý

---

(2) Odňatím slobody na jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a spôsobí ním väčšiu škodu.
(3) Odňatím slobody na tri roky až desať rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) a spôsobí ním značnú škodu,
b) z osobitného motívu,
c) závažnejším spôsobom konania, alebo
d) na chránenej osobe.
(4) Odňatím slobody na desať rokov až pätnásť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a) a spôsobí ním škodu veľkého rozsahu,
b) ako člen nebezpečného zoskupenia, alebo
c) za krízovej situácie.
Zakony pre ludi.sk. [online]. [cit. 14.06.2019]. Dostupné na internete: <https://www.zakonypreludi.sk/zz/2005-300>.
ČENTÉŠ, J. a kol., 2016. *Trestný zákon - Veľký komentár,* s. 450 a nasl.

[7] Bližšie pozri: Analýza trestnej činnosti CEO podvodov v Slovenskej republike.

[8] Pozn. autorky: Ide o osoby prostredníctvom ktorých sú zriaďované účty alebo prostredníctvom ktorých sa prevádzajú finančné prostriedky pochádzajúce z trestnej činnosti.
Bližšie pozri: Správa o vývoji trestnej činnosti CEO podvodov na území Slovenskej republiky.

komunikoval zo zahraničia a prevažne elektronickou formou. V živých prípadoch sú výsledky vyšetrovania do veľkej miery závislé od výsledkov medzinárodnej spolupráce a pomoci. K hlavným príčinám neobjasňovania týchto prípadov môžeme jednoznačne zaradiť ich medzinárodný aspekt a moderné spôsoby zakrývania totožnosti páchateľa prostredníctvom elektronickej komunikácie. Vzhľadom na tieto aspekty CEO podvodov sú lokálne možnosti objasňovania jednotlivých nižších policajných zložiek s najväčšou pravdepodobnosťou nepostačujúce.

Je evidentné, že škody spôsobené CEO podvodmi vykazujú vysoké sumy, pričom v roku 2018 v Slovenskej republike dosiahla škoda nimi spôsobená hodnotu vyše 405 000 €. V porovnaní s predchádzajúcim rokom zistená škoda bola vyššia, tak pri dokonaných činoch, ako aj pri činoch v štádiu pokusu. Celková výška škody je samozrejme ovplyvnená najmä počtom prípadov. Z uvedeného dôvodu je pre objektívnejšie posúdenie vhodné vyhodnotenie aj takzvanej škodovosti (t. j. priemernej výšky škody v jednom prípade). Vyplývajúc z uvedeného, v roku 2018 v Slovenskej republike bola pri pokuse CEO podvodu zistená škodovosť menej ako 39 000 € na jeden prípad a v dokonaných CEO podvodoch vo výške mierne prevyšujúcej 27 000 € na jeden prípad. V roku 2017 vykazovala škodovosť pri pokuse aj pri dokonaných CEO podvodoch nižšie sumy v porovnaní s rokom 2018. Z uvedeného je možné vyvodiť záver, že v ostatnom roku páchatelia vykonali menej pokusov aj dokonaných skutkov CEO podvodov v porovnaní s rokom 2017, avšak škodovosť stúpla tak pri pokusoch ako aj pri dokonaných prípadoch.[9]

Páchatelia CEO podvodov sa v minulosti zameriavali na väčšie množstvo subjektov s nižšou požadovanou sumou, a to pravdepodobne s cieľom nevzbudzovať pozornosť, respektíve neupozorňovať na seba neobvykle vysokými sumami/faktúrami. V poslednej dobe je možné konštatovať, že tento vývoj sa začína meniť – páchatelia konajú tak, že aj pri podvedení menšieho počtu subjektov získavajú väčšie množstvo podvodne vylákaných finančných prostriedkov. Vyplývajúc z analýzy slovenských dokumentov, v súvislosti s modusom operandi je možné poznamenať, že v poslednej dobe páchatelia tejto trestnej činnosti používali v zásade iba elektronickú komunikáciu (e-mail), v rámci ktorej s poškodeným/obeťou komunikovali. Prípady CEO podvodov formou telefonátu alebo správy zaslanej faxom zaznamenané neboli. Vyplývajúc z analýzy takýchto podvodov, údaje o spôsobe akým páchateľ komunikoval s poškodeným nasvedčujú tomu, že vo viacerých prípadoch sa mohlo jednať o konanie jedného páchateľa, prioritne sa zameriavajúceho na objekty v rámci Slovenskej republiky, a to z dôvodu jazykovej bariéry.

Je možné dať do pozornosti aj takzvané *sociálne inžinierstvo* ako spôsob získavania dôverných informácií pomocou manipulácie. Táto metóda bežne využíva internetovú alebo telefónnu komunikáciu, pričom zneužíva dôverčivosť ľudí vydávaním sa za známe a existujúce spoločnosti alebo inštitúcie. Útoky za využitia sociálneho inžinierstva môžu byť heterogénne, od hromadných phishingových e-mailov až po cielené, viacvrstvové a sofistikované útoky s využitím viacerých techník. Všetky však majú spoločné to, že sa zameriavajú na manipuláciu bežných spôsobov ľudského správania sa, pričom existuje iba obmedzená množina technických opatrení na ochranu pred týmito útokmi.

Objektmi, ktoré sú zo strany páchateľov najčastejšie napádané CEO podvodmi sú právnické osoby. V roku 2018 bolo najviac napadnutých obchodných spoločností založených formou s. r. o. (spoločnosť s ručením obmedzeným). Napadnuté boli aj akciové spoločnosti ale aj verejné inštitúcie (napríklad mestský úrad, centrum sociálnych služieb či

[9] Bližšie pozri: Správa o vývoji trestnej činnosti CEO podvodov na území Slovenskej republiky. Analýza trestnej činnosti CEO podvodov v Slovenskej republike.

poľnohospodárske družstvo). Dva z najčastejšie napádaných objektov (s. r. o. a verejné inštitúcie) je možné zaradiť k najzraniteľnejším z dôvodu ľahko verejne prístupných údajov o štruktúre spoločnosti a možno aj nedostatočného prístupu k informačnej bezpečnosti. V zmysle právnej formy podnikania právnických osôb v podobe obchodných spoločností typu spoločnosť s ručením obmedzeným a akciová spoločnosť, je podiel poškodených subjektov daný jednak ich početne najvyšším zastúpením v Slovenskej republike a tiež tým, že v ich prípade ide o bežné a pomerne frekventované obchodovanie, najmä s tovarom. V prípade verejných inštitúcií (či štátnych podnikov) bolo možné aj zlyhanie zodpovedného pracovníka (z dôvodu nedostatočnej skúsenosti). Určitú rolu mohla zohrať aj skutočnosť, že obchodovanie týchto subjektov je skôr výnimočné. Pri objektoch CEO podvodu sa prejavil efekt ekonomicky aktívneho regiónu (napríklad bratislavský, nitriansky či žilinský) a väčšej koncentrácie spoločností s obchodným potenciálom vhodným pre páchateľov tohto typu podvodu.[10]

Vo všeobecnosti sú samotné CEO podvody zamerané prevažne na súkromné firmy, ale aj na štátne inštitúcie či verejné organizácie, v rámci ktorých sú bežne vykonávané elektronické bankové prevody na pokyn nadriadených (takzvaných CEO manažérov). Jednou z *foriem* je, že útočník, ktorý disponuje internými informáciami o spôsobe fungovania organizácie, tieto zmanipuluje a vydávajúc sa za CEO manažéra osloví objekt (pracovníka účtárne alebo účtovníka) s požiadavkou na prevod finančných prostriedkov.

Na základe informácií získaných z už spáchaných CEO podvodov aj v zahraničí, je možné pozorovať viaceré metódy/spôsoby (pôsobiace jednotlivo alebo aj vzájomným prelínaním sa) využívané ich páchateľmi:

a) Pozmenená faktúra - je využívaná pri spoločnostiach, ktoré spolupracujú najmä s dodávateľmi zo zahraničia. Páchateľ vydávajúc sa za klienta (dodávateľa), kontaktuje (poškodenú) spoločnosť /telefonicky, e-mailom, faxom/, pričom požiada jej pracovníka o zmenu čísla účtu, na ktorý má byť platba za faktúru zaslaná. Ide o už existujúcu faktúru za obchod, ktorý práve prebieha.
b) Falošný manažér - páchateľ, ktorý sa vydáva na CEO manažéra inštruuje (napríklad telefonicky alebo e-mailom) pracovníka (poškodenej) spoločnosti k vykonaniu prevodu finančných prostriedkov na určený účet z dôvodu akútnej a neodkladnej potreby vykonania takejto transakcie.
c) Falošný e-mail - páchateľ vytvorí falošnú e-mailovú adresu totožnú s e-mailovou adresou CEO manažéra, z ktorej sú následne rozposielané falošné faktúry poškodeným spoločnostiam, pričom ide o spoločnosti, s ktorými spoločnosť falošného CEO manažéra obchoduje alebo obchodovala – ide o faktúry za obchod, ktorý reálne neprebehol.
d) Falošný advokát - spôsob, pri ktorom páchateľ kontaktuje zamestnanca/CEO manažéra, pričom sa vydáva za právnika zastupujúceho ich spoločnosť, s požiadavkou na okamžitú úhradu nákladov na riešenie údajného problému spoločnosti, ktorý sa rieši (napríklad súdne poplatky, dlžná suma, nedoplatky na povinných platbách). Môže tiež ísť o prípady, kedy sa páchatelia vydávajú za právnikov zastupujúcich spoločnosť CEO manažéra a v jeho mene uplatnia právo (napríklad vo forme exekučného príkazu) voči inej spoločnosti.[11]

V roku 2018 sa v Slovenskej republike *modus operandi* CEO podvodov ustálil v dvoch základných formách využívaných páchateľmi:

[10] Bližšie pozri: Správa o vývoji trestnej činnosti CEO podvodov na území Slovenskej republiky. Analýza trestnej činnosti CEO podvodov v Slovenskej republike.
[11] Bližšie pozri: Analýza trestnej činnosti CEO podvodov v Slovenskej republike.

a) Maskovaný e-mail - spôsob, v rámci ktorého si páchateľ vytvorí e-mailovú adresu, ktorej hlavička sa zobrazuje pod vybraným tvarom a ten sa zhoduje s tvarom e-mailu CEO manažéra, za ktorého sa páchateľ vydáva.
b) Phishingový útok - spôsob získavania osobných a bezpečnostných údajov (prístupových hesiel), ktorý páchateľovi umožňuje vstúpiť do obchodnej/pracovnej komunikácie medzi CEO manažérom a účtovníkom za použitia pravej e-mailovej adresy CEO manažéra.

Rozdiel medzi uvedenými formami tkvie najmä v rozsahu odborných znalostí páchateľov a ich samotnom prevedení. Vytvorenie maskovanej e-mailovej adresy si vyžaduje menšie počítačové zručnosti v porovnaní s realizáciou CEO podvodu formou phishingu. Navyše, návodov na realizáciu je v rámci internetu dohľadateľných mnoho. Páchateľ si následne vytypuje z dostupných zdrojov inštitúciu, ktorá má potrebné e-mailové adresy zverejnené a osloví (potenciálneho) poškodeného/obeť so žiadosťou o rýchly prevod finančných prostriedkov do zahraničia. V prípade phishingového útoku je predpokladom páchateľa preniknutie do počítačového systému potenciálneho poškodeného/obete. Vyplývajúc z toho disponuje údajmi o jeho komunikácii, obchodných aktivitách, vnútornom fungovaní spoločnosti a vo viacerých prípadoch aj údajmi z dostupných sociálnych sietí. Tieto páchateľ využíva pre účel adresného a aj časovo presného koordinovania svojho útoku - napríklad neprítomnosť CEO manažéra na pracovisku či zmena čísla účtu na faktúre v už prebiehajúcej obchodnej operácii. Uvedená metóda zvyšuje úspešnosť samotného CEO podvodu, na strane druhej si vyžaduje omnoho väčšie odborné znalosti, v porovnaní s formou maskovaného e-mailu, keďže ide o cielený sofistikovaný útok. Pri tejto metóde býva následne použitá pozmenená faktúra (resp. číslo účtu) v už prebiehajúcom obchode.

Z celkového počtu prípadov zaznamenaných v roku 2018 v Slovenskej republike väčšina bola realizovaná formou maskovaného e-mailu a iba v dvoch prípadoch bola využitá metóda phishingu. V porovnaní s predchádzajúcim rokom, kedy dominoval spôsob CEO podvodu formou phishingu a až následne metódou maskovaného e-mailu, došlo k zmene. Predpokladom dôvodu zmeny je, že potenciálne objekty dbajú na dôslednejšie zabezpečenie svojho softvéru pred neoprávneným vstupom do obchodnej komunikácie čím páchateľom znemožňujú vykonanie podvodu.

Modus operandi páchateľov takýchto podvodov ide ruka v ruke s *etiológiou* CEO podvodov. Je faktom, že pred prijímaním podvodných e-mailov nie je možné sa softvérovo až tak účinne brániť, a tak dokonanie skutku je často spôsobené (aj následným) zlyhaním ľudského faktora. Je možný aj výskyt nedostatočného oboznámenia zodpovedných osôb s existenciou spomenutých protiprávnych konaní či nedostatočného preventívneho pôsobenia CEO manažérov. Bolo by na mieste dbať na štandardné bezpečnostné (administratívne) postupy, najmä pri udeľovaní pokynov na akýkoľvek prevod alebo platbu finančných prostriedkov, predovšetkým na zahraničné účty, napríklad v podobe dvojitej kontroly, telefonického overenia pri náhlej požiadavke o úhradu alebo pri náhlej zmene čísla účtu na faktúre. Slovenská republika patrí do skupiny krajín (spolu napríklad s Českou republikou, Poľskou republikou či Maďarskou republikou), cez ktoré sa realizuje skôr tranzit finančných prostriedkov z takýchto prípadov spáchaných v zahraničí. Z etiologického pohľadu je tento stav dôsledkom legislatívnych medzier (najmä v oblasti finančného trhu), ktoré sú páchateľmi využívané v rámci prevodov finančných prostriedkov realizovaných medzi štátmi Európskej únie. Vo väčšine prípadov potrebuje páchateľ účet v banke, ktorý bude mať pod kontrolu aj napriek tomu, že nebude jeho majiteľom. Na tento účel sú organizovaní rôzni sprostredkovatelia, ktorí či už za úplatu alebo podvodom, zriadia účet a následne poskytnú k nemu prístupové práva páchateľom CEO podvodov alebo na ich pokyn vykonajú príslušné transakcie. Účelové zakladanie účtov sa tak v Slovenskej republike (ale nie len) stalo, najmä

pre cudzincov, lukratívnym zdrojom príjmov, pričom v súčasnosti nie je možné hovoriť o účinných opatreniach výraznejšie tomu brániacich.[12]

V súvislosti s CEO podvodmi a vzhľadom na následné konanie páchateľov je na mieste uviesť, že ide aj o predikatívny trestný čin k následnej legalizácii nimi získaného príjmu z trestnej činnosti.[13] Teda CEO podvody vo veľkej miere súvisia s *legalizáciou príjmov z trestnej činnosti*[14]. Výročná správa finančnej spravodajskej jednotky za rok 2018 uvedené potvrdzuje tým, že z analýzy hlásení neobvyklých obchodných operácií[15] vyplynulo, že medzi najčastejšie prípady legalizácie príjmov z trestnej činnosti a ich naviazaniu na predikatívnu trestnú činnosť, v roku 2018 patrili okrem iných aj podvody – konkrétne CEO podvody.[16] Práve trestný čin legalizácie príjmu z trestnej činnosti je prvkom, ktorý spája prípady vykazujúce znaky CEO podvodu, pretože spôsob, akým páchateľ realizuje prevod získaných finančných prostriedkov a ich následný výber, je zároveň najväčšou slabinou v spletitej štruktúre CEO podvodov. Dôležitú úlohu v týchto prípadoch zohráva doba od vylákania finančných prostriedkov až po ich postupný prevod na účet páchateľa, respektíve následný prevod na iné účty.[17]

Spôsobov (metód), ktorými je možné legalizovať príjmy z trestnej činnosti je mnoho. Metóda legalizácie predstavuje postup organizovanej skupiny alebo jednotlivca na dosiahnutie cieľa, ktorým je vytvorenie zdania legálneho pôvodu majetku, ktorý bol v skutočnosti získaný trestnou činnosťou. Využitie konkrétnej metódy je závislé od dvoch faktorov, od takzvanej „zdrojovej kriminality“ a od podoby majetku/príjmu získaného trestnou činnosťou. Prvým spomenutým faktorom, zdrojovou kriminalitou, je nazerané na to z akého trestného činu bol získaný majetok/príjem. Teda či zdrojový trestný čin bol spáchaný organizovanou skupinou alebo jednotlivcom a či napríklad súvisel s drogovou kriminalitou, všeobecnou kriminalitou, ekonomickou alebo finančnou kriminalitou, či sa jednalo o prostú alebo vysoko sofistikovanú kriminalitu. Podoba majetku/príjmu získaného trestnou činnosťou, je druhým spomenutým faktorom, z ktorého vyplýva, že iným spôsobom sa bude legalizovať majetok, ktorý má podobu peňazí, iným hnuteľná vec, nehnuteľnosť, duševné vlastníctvo a podobne. Vyplývajúc z týchto súvislostí môžeme konštatovať, že nie je možné poskytnúť vyčerpávajúci zoznam metód legalizácie príjmov z trestnej činnosti. Dôvodmi vzniku nových metód/spôsobov legalizácie príjmov z trestnej činnosti sú najmä sofistikácia páchania zdrojovej kriminality a zvyšujúca sa flexibilita organizovaných skupín. Za zmienku stoja aj nové spôsoby realizácie obchodných transakcií – zrýchľujú a zdokonaľujú sa, a to za

---

[12] Bližšie pozri: Správa o vývoji trestnej činnosti CEO podvodov na území Slovenskej republiky.
Analýza trestnej činnosti CEO podvodov v Slovenskej republike.

[13] V podmienkach Slovenskej republiky môže v odôvodnených prípadoch na CEO podvody nadväzovať (s nimi súvisieť) aj trestný čin podielnictva (podľa § 231 a 232 TZ).
Bližšie pozri: Analýza trestnej činnosti CEO podvodov v Slovenskej republike.
Zakony pre ludi.sk. [online]. [cit. 14.06.2019]. Dostupné na internete: <https://www.zakonypreludi.sk/zz/2005-300>.

[14] Legalizácia príjmu z trestnej činnosti, § 233 a 234 TZ.
Zakony pre ludi.sk. [online]. [cit. 14.06.2019]. Dostupné na internete: <https://www.zakonypreludi.sk/zz/2005-300>.
Pozn. autorky: viac pozri aj v – Zákon č. 297/2008 Z. z. Zákon o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov.
Zakony pre ludi.sk. [online]. [cit. 14.06.2019]. Dostupné na internete: <https://www.zakonypreludi.sk/zz/2008-297>.

[15] Pozn. autorky: bližšie pozri § 4 zákona č. 297/2008 Z. z. Zákon o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov.
Zakony pre ludi.sk. [online]. [cit. 14.06.2019]. Dostupné na internete: <https://www.zakonypreludi.sk/zz/2008-297>.

[16] Bližšie pozri: Výročná správa finančnej spravodajskej jednotky za rok 2018.

[17] Bližšie pozri: Analýza trestnej činnosti CEO podvodov v Slovenskej republike.

využitia nových metód bankových transakcií. Vyplývajúc z doterajšej aplikačnej praxe je možné hovoriť napríklad o týchto najčastejšie využívaných metódach legalizácie príjmov z trestnej činnosti – umelé zvyšovanie obratu pri firmách pracujúcich s hotovosťou; umelé zvyšovanie obratu alebo zisku nadmernou fakturáciou; metóda spätnej pôžičky; pôžička typu back-to-back; fingované výhry; medzinárodné peňažné prevody; bankové šeky, zmenky, akreditívy, kapitálové vklady; transakcie s nehnuteľnosťami; „krádeže“ identity (z identifikačných dokladov, platobných kariet, skimming, phishing;[18] takzvané *CEO podvody*.[19]

Dôležitým faktorom, ktorý v mnohom predchádza samotnému CEO podvodu je existencia respektíve zriadenie bankového účtu kde budú poukazované podvodne vylákané finančné prostriedky. Tento účet je otvorený v banke s domicilom spravidla v inej krajine ako v tej, v ktorej je dislokovaný účet odosielateľa platby – obchodného partnera. Na tento účel sú vo všeobecnosti využívané takzvané „money mule“. Tieto osoby sú najčastejšie oslovené elektronickou formou, nie zriedka pod zámienkou pracovnej ponuky alebo formou služby za odplatu. Teda v prípade CEO podvodov spáchaných v Slovenskej republike je pravidlom, že finančné prostriedky sú prevádzané na účty založené v zahraničí. Využívanie tohto spôsobu výrazne ovplyvňuje možnosti zaistenia finančných prostriedkov. Zároveň slúži k zmareniu identifikácie útočníka, prípadne konečného príjemcu finančných prostriedkov. Vo väčšine prípadov sú finančné prostriedky prevádzané aj niekoľkokrát, kým skončia na účte, z ktorého sú následne vyberané v hotovosti – konečným príjemcom (páchateľom) alebo ďalšou „money mule“, ktorá ich odovzdá páchateľovi alebo následne zasiela páchateľovi (napríklad cez službu Western Union alebo iné). Vo fáze bezhotovostných prevodov dochádza k ich realizácii (k samotným prevodom peňazí) na ďalšie vopred páchateľom pripravené účty vedené v bankách s domicilom v offshore krajinách alebo krajinách so sťaženým uplatňovaním vymožiteľnosti práva, ako napríklad Nigéria, Čína, Ghana či Hongkong. Často dochádza k bezhotovostným prevodom aj na účty vedené v bankách s domicilom vo Veľkej Británii, pričom je možné upriamiť pozornosť na indície, že tieto účty sú zakladané pre osoby, ktoré v rámci migrácie obyvateľstva z tretích krajín získali azyl vo Veľkej Británii a sú využívané v tejto veci páchateľmi v pozícii takzvaných bielych koní. Z analýzy CEO podvodov (v rámci ktorých boli zistené údaje o bankových účtoch) v Slovenskej republike v roku 2018 bolo zistené v 69% prípadov smerovanie finančných prostriedkov na účty založené vo Veľkej Británii. Druhou najčastejšie využívanou krajinou pre tento účel bola Ukrajina. Ku krajinám, v ktorých boli alebo mali byť legalizované finančné prostriedky pochádzajúce z trestnej činnosti CEO podvodov, môžeme zaradiť aj Španielske kráľovstvo, Tureckú republiku, Holandsko či Čínsku ľudovú republiku.[20]

V zmysle uplatnenia *prevencie* sa v súčasnosti ako najlepší spôsob ochrany pred CEO podvodmi javí zvyšovanie bezpečnostného povedomia fyzických aj právnických osôb (potenciálnych poškodených) pred možnosťou takéhoto konania páchateľov. Častokrát sa ale vyskytne aj „neúspech“ páchateľov CEO podvodov – najčastejším dôvodom je obozretnosť (potenciálne) dotknutých CEO manažérov a za účty zodpovedných pracovníkov spoločností. Tento „neúspech“ vychádza najmä z prehľadu o jednotlivých obchodných operáciách, prípadne z bezpečnostných opatrení vo forme dodatočného overovania alebo dvojitého schvaľovania prevodov finančných prostriedkov spoločnosti. Určitým faktorom je aj to, že

[18] Bližšie k jednotlivým metódam pozri: STIERANKA, J. a kol., 2018. Legalizácia príjmov z trestnej činnosti a financovanie terorizmu, právna a inštitucionálna ochrana v Slovenskej republike, s. 28-50.

[19] STIERANKA, J. a kol., 2018. Legalizácia príjmov z trestnej činnosti a financovanie terorizmu, právna a inštitucionálna ochrana v Slovenskej republike, s. 27 a nasl.

[20] Bližšie pozri: Správa o vývoji trestnej činnosti CEO podvodov na území Slovenskej republiky.
STIERANKA, J. a kol., 2018. Legalizácia príjmov z trestnej činnosti a financovanie terorizmu, právna a inštitucionálna ochrana v Slovenskej republike, s. 42 a nasl.

objem obchodov v rámci Slovenskej republiky je menší oproti ekonomicky silnejším krajinám (ako napríklad Francúzska republika).

Bol spracovaný aj návrh preventívnych opatrení v podobe zverejnenia výstrahy pred útokmi páchateľov CEO podvodov vo vzťahu k dostupným masovo-komunikačným prostriedkom. V októbri 2018 bola slovenská verejnosť oboznámená s výstrahou formou krátkej správy na sociálnej sieti Facebook prostredníctvom Facebooku Policajného zboru, a to uvedením konkrétneho anonymizovaného prípadu s odkazom na všeobecný popis CEO podvodu. Ešte dva mesiace predtým, v auguste 2018, bola na webovej stránke www.minv.sk doplnená sekcia „Podvodné prevody peňazí", v rámci ktorej je zverejnená výstraha pred útokom páchateľov CEO podvodov.[21]

Je tiež potrebné zamerať pozornosť na celkový prístup organizácií k informačnej bezpečnosti, dôsledné dodržiavanie bezpečnostných politík (pravidiel) a samozrejme podporovať aktívnu participáciu zamestnancov jednotlivých inštitúcií na ich bezpečnosti. Tiež samotn spracovanie „Analýzy trestnej činnosti CEO podvodov v Slovenskej republike" a „Správy o vývoji trestnej činnosti CEO podvodov na území Slovenskej republiky" napomáha najmä vykonávaním preventívnych opatrení znižovať počet zaznamenaných prípadov, či už spáchaných v štádiu pokusu alebo dokonaných činov (CEO podvodov). Čiastočne preventívny účinok má nepochybne aj Výročná správa finančnej spravodajskej jednotky za rok 2018.

Preventívny účinok by nepochybne mal aj informačný systém, ktorý by v reálnom čase poskytoval jednotlivým zložkám podrobný prehľad o výskyte tejto trestnej činnosti prierezovo v rámci celého územia Slovenskej republiky spolu s vybranými markantmi (IP adresy, text oslovenia, číslo účtu a podobne) – absencia takéhoto systému sa v tejto oblasti javí ako problematická.[22]

Je nevyhnutné poznamenať, že jednotlivé kriminologické ukazovatele (fenomenológia, etiológia, modus operandi páchateľov, poškodené objekty či prevencia) predmetnej kriminality, v danom prípade CEO podvodov, sa tak v teórii ako aj aplikačnej praxi vzájomne prelínajú.

CEO podvody v aplikačnej praxi

V septembri 2018 v dopoludňajších hodinách doposiaľ neznámy páchateľ vydávajúci sa za konateľa spoločnosti, prostredníctvom e-mailovej komunikácie (e-mailu) kontaktoval obchodnú zástupkyňu spoločnosti, ktorej dal pokyn na úhradu faktúry za objednávku z ukrajinskej firmy, vo výške viac ako 8 300 €, v prospech účtu vedenom v banke v Ukrajine. V následnej komunikácii zadal pokyn o okamžitú úhradu čiastky 3 300 € na tento účet s tým, že zvyšok nakázal uhradiť nasledujúci deň. Obchodná zástupkyňa spoločnosti v presvedčení, že bola o vykonanie uvedenej úhrady požiadaná konateľom, previedla ešte v ten istý deň z účtu spoločnosti čiastku 3 300 €. Pri následnej komunikácii s konateľom spoločnosti bolo zistené, že konateľ žiaden e-mail obchodnej zástupkyni neposlal a ani úhradu žiadnej platby

[21] Minv.sk. [online]. [cit. 14.06.2019]. Dostupné na internete: <https://www.minv.sk/?podvodne-prevody-penazi>.
Pozn. autorky: v tejto súvislosti Policajný zbor odporúča → „1. Oboznámiť zodpovedné osoby s existenciou vyššie uvedeného protiprávneho konania, prípadne prijať opatrenia za účelom pravidelných školení zameraných na aktuálne kybernetické hrozby. 2. Zavedenie technických opatrení ako aj bezpečnostných (administratívnych) postupov, pri udeľovaní pokynov na akýkoľvek prevod alebo platbu finančných prostriedkov najmä na zahraničné účty (dvojitá kontrola, telefonické overovanie pri náhlej požiadavke o úhradu alebo pri náhlej zmene čísla účtu na faktúre a pod.)."

[22] Bližšie pozri: Správa o vývoji trestnej činnosti CEO podvodov na území Slovenskej republiky.
Analýza trestnej činnosti CEO podvodov v Slovenskej republike.
Výročná správa finančnej spravodajskej jednotky za rok 2018.

od nej nežiadal. Týmto konaním bola danej spoločnosti spôsobená škoda vo výške 3 300 €. V prípade uskutočnenia prevodu aj zvyšnej čiastky sumy by bola predmetnej spoločnosti spôsobená škoda vo výške viac ako 8 300 €.[23]

Finančná spravodajská jednotka prijala v januári 2018 od povinnej osoby- Banka A hlásenie o neobvyklej obchodnej operácii týkajúcej sa dvoch podvodných platieb smerujúcich od dvoch zahraničných spoločností B a C z účtov vedených v Nemecku v celkovej sume 178 000,- €. Obidve zahraničné platby boli v rovnakej sume 89 000,- € a boli pripísané na ten istý účet vedený Bankou A pre osobu D. Zahraničná banka žiadala vrátiť tieto finančné prostriedky späť na zahraničné účty spoločností B a C z dôvodu podvodu a zaslala aj kópiu trestného oznámenia. Nakoľko sa banka o podvodných platbách dozvedela včas, ešte pred nakladaním s finančnými prostriedkami, vykonala technické opatrenia na účte osoby D a po pokuse o nakladanie s finančnými prostriedkami na účte osoby D prostredníctvom služby Internetbanking následne pristúpila k zdržaniu v zmysle § 16 zákona o ochrane pred legalizáciou.

Analýzou hlásenia o neobvyklých obchodných operáciách bolo zistené, že prevodu obidvoch vyššie uvedených zahraničných platieb zo zahraničných účtov predchádzalo „hacknutie“ elektronickej obchodnej komunikácie majiteľa zahraničných účtov subjektov B a C a pôvodné platby boli presmerované na nesprávny účet patriaci osobe D.

Finančná spravodajská jednotka následne spracovala informáciu, ktorú odstúpila príslušnému orgánu činnému v trestnom konaní, ktorý na základe tejto informácie začal trestné stíhanie pre obzvlášť závažný zločin legalizácie príjmov z trestnej činnosti v štádiu pokusu. Prokuratúra následne zaistila na účte osoby D peňažné prostriedky v celkovej hodnote 178 000,- €.[24]

Závery

V závere je možné, na základe relatívne nízkeho počtu zistených prípadov a klesajúceho trendu zistených CEO podvodov (v porovnaní s minulým obdobím), konštatovať že Slovenská republika nie je bezprostredne a trvalo ohrozená touto trestnou činnosťou.

V zmysle účinného uplatňovania kontroly kriminality v nasledujúcom období je/bude na mieste naďalej sledovať vývoj CEO podvodov v rámci Slovenskej republiky.

Spolupráca na medzinárodnej a národnej úrovni je neopísateľne dôležitou v celom procese odhaľovania a objasňovania CEO podvodov. V Slovenskej republike v rámci služobnej spolupráce ide predovšetkým o kooperáciu týchto útvarov: odbory kriminálnej polície krajských a okresných riaditeľstiev Policajného zboru, Úrad kriminálnej polície Policajného zboru, NAKA P PZ, odbor počítačovej kriminality úradu kriminálnej polície Prezídia Policajného zboru a i. Dôležitým je aj oboznamovanie príslušných útvarov s aktuálnym stavom a vývojom CEO podvodov, ktoré je realizované predovšetkým správou o vývoji trestnej činnosti CEO podvodov na území Slovenskej republiky (spracovanou úradom kriminálnej polície Prezídia Policajného zboru). V zmysle medzinárodnej spolupráce vo veci preverenia výskytu bankových účtov zistených v prípadoch CEO podvodov spáchaných v rámci územia Slovenskej republiky je úvahou, aby táto prebiehala aj s národnou ústredňou Europolu úradu medzinárodnej policajnej spolupráce Prezídia Policajného zboru. Finančná spravodajská jednotka, ktorej zámerom je záujem (okrem iných) aj o CEO podvody, je aktívnym členom medzinárodných orgánov, ako je napríklad aj výbor Moneyval. Uvedené potvrdzuje medzinárodný rozmer predmetnej problematiky a následne aj nevyhnutnosť medzinárodnej policajnej či právnej spolupráce.

[23] Bližšie pozri: Správa o vývoji trestnej činnosti CEO podvodov na území Slovenskej republiky.
[24] Bližšie pozri: Výročná správa finančnej spravodajskej jednotky za rok 2018.

V roku 2018 sa v Slovenskej republike nepodarilo objasniť ani jeden prípad CEO podvodu. V porovnaní s rokom 2017 došlo v roku 2018 k zníženiu počtu zistených CEO podvodov. V rokoch 2013 – 2016 bolo možné pozorovať stagnujúcu tendenciu. V roku 2017 došlo k relatívne výraznému nárastu (na viac ako dvojnásobok) zaznamenaných CEO podvodov (v porovnaní s rokom 2016). Modus operandi páchateľov bol vo väčšine prípadov maskovaný e-mail, v porovnaní s využitím náročnejšieho spôsobu realizácie - phishingom, ktorý bol využitý iba v dvoch prípadoch. Páchatelia sa zameriavali na menšie množstvo subjektov, avšak s vyššou požadovanou sumou. Teda škodovosť bola vyššia. Objektmi CEO podvodov sa v najväčšej miere stali právnické osoby založené vo forme spoločností s ručením obmedzeným a akciových spoločností, výnimkou neboli ani štátne inštitúcie. Finančné prostriedky pochádzajúce z CEO podvodov v Slovenskej republike boli prevedené do zahraničia, najčastejšie na účty vo Veľkej Británii. Finančné vyšetrovanie sa nevykonávalo ani v jednom prípade CEO podvodu.

Výročná správa finančnej spravodajskej jednotky za rok 2018 upriamuje pozornosť na predpoklad nárastu CEO podvodov v roku 2019, nakoľko neexistujú (reálne funkčné) prevenčné opatrenia smerujúce k ich zamedzeniu. Predchádzať takýmto podvodom možno aj (okrem iného) snahou o dôslednú a neustálu kontrolu údajov uvádzaných v dokumentoch/dokladoch v rámci realizácie obchodného vzťahu dvoch partnerských spoločností. Zároveň výročná správa finančnej spravodajskej jednotky za rok 2018 upriamuje pozornosť na prognózy ďalšieho vývoja na úseku legalizácie a financovania terorizmu, kde konštatuje, že na základe analýzy doterajšieho vývoja trendov v oblasti legalizácie a financovania terorizmu, za súčasného zohľadnenia získaných informácií, existujúcich okolností a aktuálnych udalostí v Slovenskej republike, možno v nasledujúcom období predpokladať generovanie príjmov: napríklad páchaním majetkovej trestnej činnosti formou internetových podvodov a takzvaných *CEO podvodov*; páchaním rôznych aj nových foriem daňovej trestnej činnosti; využívaním daňových rajov a offshore spoločností a zapájanie schránkových a fiktívnych spoločností do zložitých obchodných schém a podobne.[25]

Literatúra

Analýza trestnej činnosti CEO podvodov v Slovenskej republike. Úrad kriminálnej polície Prezídia Policajného zboru.

ČENTÉŠ, Jozef a kol., 2016. *Trestný zákon - Veľký komentár*, 3. aktualizované vydanie. Žilina: Eurokódex, s. r. o., 959 s. ISBN 978-80-8155-066-9.

Europol.europa.eu. [online]. [cit. 11.06.2019]. Dostupné na internete:
<https://www.europol.europa.eu/crime-areas-trends/europol-analysis-projects>.

Minv.sk. [online]. [cit. 14.06.2019]. Dostupné na internete:
<https://www.minv.sk/?podvodne-prevody-penazi>.

Správa o vývoji trestnej činnosti CEO podvodov na území Slovenskej republiky v roku 2018. Úrad kriminálnej polície Prezídia Policajného zboru.

STIERANKA, Jozef a kol., 2018. *Legalizácia príjmov z trestnej činnosti a financovanie terorizmu, právna a inštitucionálna ochrana v Slovenskej republike*. Bratislava: Wolters Kluwer SR, s. r. o.,193 s. ISBN 978-80-8168-912-3.

Zakony pre ludi.sk. [online]. [cit. 14.06.2019]. Dostupné na internete:
<https://www.zakonypreludi.sk/zz/2005-300>.

[25] Bližšie pozri: Výročná správa finančnej spravodajskej jednotky za rok 2018.
Správa o vývoji trestnej činnosti CEO podvodov na území Slovenskej republiky.
Analýza trestnej činnosti CEO podvodov v Slovenskej republike.

Zakony pre ludi.sk. [online]. [cit. 14.06.2019]. Dostupné na internete: <https://www.zakonypreludi.sk/zz/2008-297>.
Výročná správa finančnej spravodajskej jednotky za rok 2018. Finančná spravodajská jednotka národnej kriminálnej agentúry Prezídia Policajného zboru Ministerstva vnútra Slovenskej republiky.

Keywords: fraud, CEO (Chief Executive Officer) fraud, money laundering, unusual business operation, Bureau of Criminal Police of the Police Force Presidium, Financial Intelligence Unit of the National Crime Agency of the Police Force Presidium, Slovak Republic.

Summary

The main aim of the article is to analyse CEO frauds. It is a relatively new and a serious form of crime. CEO frauds are associated with unusual business operations and with money laundering. They are considered as predictive crimes. The article analyses CEO frauds from the view of criminology (phenomenology, etiology, modus operandi of perpetrators, damaged objects, prevention) in the theoretical part. In the empirical part of the article two recent real cases from police practice are analysed. The main sources of information were obtained from the Bureau of Criminal Police of the Police Force Presidium, Unit of the National Crime Agency of the Police Force Presidium, professional literature and legal documents.

mjr. JUDr. Michaela Jurisová, PhD.
Katedra kriminológie
Akadémia Policajného zboru v Bratislave
Tel.: 0961057113
e-mail: michaela.jurisova@minv.sk

Recenzent: prof. Ing. Jozef Stieranka, PhD.