**KRÍZOVÝ MANAŽMENT**
DOI 10.26552/krm.C.2021.2.39-46
ISSN 1336 - 0019

# ŠPECIFIKÁ PODVODU TYPU „CEO“

## SPECIFICS OF „CEO“ FRAUDS

MICHAELA JURISOVÁ

**ABSTRACT:** *The article deals with a specific type of fraud – Chief Executive Officer Fraud – CEO Fraud. This crime also grows in the Slovak Republic. Its specifics are the presence of a false manager, sophistication of perpetrators, international dimension, deceiving the accountant, masked email, „money mule“, money laundering, extensive financial damage, social engineering, etc. The text contains information about the situation in the Slovak Republic, mainly in 2020. The article also includes recommendations and prevention options*

**KEYWORDS:** *Fraud. CEO Fraud – Chief Executive Officer Fraud. False manager. Money laundering. Money mule.*

## ÚVOD

Kriminalita (zločinnosť) ako najzávažnejší, hromadný sociálno-patologický / sociálno-právny jav (fenomén) je predmetom skúmania mnohých vedných odborov a predmetov (napríklad aj študijného odboru Ochrana osôb a majetku). Účelom je ochrana spoločnosti pred negatívnymi protispoločenskými javmi, rôznymi druhmi trestnej činnosti, pred organizovanou kriminalitou alebo aj pred terorizmom. Cieľom príspevku je informovať čitateľa o špecifickom druhu podvodu, ktorého prienik je zjavný už aj v Slovenskej republike. Želaním je, aby získané poznatky a informácie obohatili expertov na túto oblasť (z radov teoretikov ako aj odborníkov z aplikačnej praxe) a samozrejme aj laikov. V dnešnom uponáhľadom svete môže byť potenciálnym poškodeným (obeťou) teoreticky každý z nás. Obzvlášť v súlade so stále narastujúcim špecifikom kriminality – a to presunom z reálneho do virtuálneho prostredia.

Evidentným faktom je, že zaoberať sa bezpečnosťou jednotlivých oblastí spoločenského a hospodárskeho života je nevyhnutné. Nie však separátne. Uvedené by bolo nedostatočné. Prítomná je potreba celostného (holistického) chápania bezpečnosti. Preto zložitý komplex otázok, týkajúcich sa rozličných aspektov bezpečnosti si vyžaduje multidisciplinárny prístup k otázkam a obsahu bezpečnostného výskumu, bez ktorého nie je možné čeliť súčasným i budúcim bezpečnostným výzvam. Zároveň je možné súhlasiť s Hofreiterom - o potrebe a význame teórie pre bezpečnostné vzdelávanie. Bezpečnosť sama o sebe je zložitý, vnútorne štruktúrovaný, multifaktorový a hierarchizovaný fenomén, ktorého obsah, štruktúra i funkcie presahujú hranice nielen jedného vedného odboru (napríklad policajná veda, vojenská veda) ale dokonca i celých vedných oblastí (spoločenských, prírodných, technických a i.). Obzvlášť v kontexte formovania policajných vied je teória definovaná ako systém zovšeobecnených objektívne pravdivých poznatkov alebo systém poznaktov odvodených z iných teórií. V procesoch zaisťovania bezpečnosti človek vystupuje v role subjektu. Táto rola vyžaduje zvládnutie širokého spektra poznatkov, zákonov, požiadaviek, metód riešenia problémov bezpečnosti. Človek, ako hlavný subjekt bezpečnosti potrebuje na plnenie svojej roly poznatky, znalosti, metodické a iné nástroje. Potrebuje teóriu. Prikláňam sa k formulácii, že vedecká teória je súborom vedeckých poznatkov, tvrdení o týchto poznatkoch usporiadaných takým spôsobom, ktorý umožňuje ich použitie pri explanácii a predikcii javov a udalostí, majúcich rozhodujúci vplyv na vývoj v danej sfére reality (Hofreiter, 2019). Pri vedeckom skúmaní je nevyhnutné relektovať na fakt, že táto zložitá, zámerná, analyticko-syntetická a intelektuálno-poznávacia činnosť vychádza z praxe a vracia sa späť do praxe. Predmetný príspevok bol podporený využitím heterogénnych metód a techník skúmania.

**CEO podvody** (z anglického *Chief Executive Officer Frauds*) neobchádzajú ani Slovenskú republiku, pričom je zároveň možné predpokladať, že sa čoraz viac dostávajú do povedomia odbornej aj laickej verejnosti. Ide o špecifické podvody páchané prostredníctvom pokynov falošných / fiktívnych manažérov.

CEO podvod predstavuje cielený útok – pointou ktorého je oklamanie zamestnanca zvyčajne z finančného alebo účtovníckeho oddelenia. Pri realizácii samotného podvodu je vyvíjaný tlak na zamestnanca spoločnosti, aby previedol značné sumy peňazí (predovšetkým do zahraničia). Tieto podvody sú spájané so sociálnym inžinierstvom. Podvodníci využívajú jeho klasické triky, a to prostredníctvom verejne dostupných internetových stránok, ale aj „nabúraním sa“ do e-mailovej komunikácie príslušnej spoločnosti. Zistia údaje o prebiehajúcich obchodoch a kontaktoch, ako aj o spôsoboch komunikácie a samotnej identitie CEO manažéra či zodpovedného zamestnanca za prevody peňazí. Páchatelia následne (vydávajúc sa za CEO manažéra), kontaktujú príslušného zamestnanca, aby uskutočnil finančnú transakciu. Toto prebieha najčastejšie prostredníctvom e-mailu alebo telefonicky. Účelom je navodenie atmosféry časovej tiesne. Falošný manažér v rámci takejto komunikácie „nedá svojmu podriadenému na výber“. Komunikácia je realizovaná formou striktných pokynov a často aj v spojitosti s hrozbou sankcie za nesplnenie pokynu. Po prevode peniaze skončia v inom štáte, kde sú ďalej „prepierané“. Základný model tohto podvodu zahŕňa minimálne dva štáty (často členské štáty Európskej únie). Prítomnými bývajú aj takzvané „money mule“ – osoby, prostredníctvom ktorých sú zriaďované účty alebo prevádzané finančné prostriedky pochádzajúce z trestnej činnosti. Pri týchto podvodoch ide v podstate o „podvod s platobným príkazom“ namiereným najmä voči spoločnostiam, ale aj súkromným osobám alebo štátnym inštitúciám. Škody spôsobené takýmito podvodmi sú veľmi vysoké (Jurisová, 2021; Jurisová, 2020).

Možný priebeh CEO podvodu naznačuje Obrázok 1. Načrtáva časový sled jednotlivých krokov páchateľov aj typické prvky ich konania.


Obrázok 1 Ako prebieha CEO podvod (Europol, 2020)

V zmysle slovenskej legislatívy sú CEO podvody kvalifikované ako trestný čin podvodu podľa § 221 Trestného zákona. Môže ísť aj o súbeh trestného činu podvodu a trestných činov počítačovej kriminality podľa § 247 a nasl. Trestného zákona alebo legalizácie výnosu z trestnej činnosti podľa § 233 Trestného zákona (Jurisová, 2020(a); Marková, 2018; Stieranka, 2018).

Podvodom je ak niekto na škodu cudzieho majetku seba alebo iného obohatí tým, že uvedie niekoho do omylu alebo využije niečí omyl, a spôsobí tak na cudzom majetku škodu (Čentéš, 2020).

# 1. PODVODY PÁCHANÉ PROSTREDNÍCTVOM PRÍKAZOV FALOŠNÝCH MANAŽÉROV V PODMIENKACH SLOVENSKEJ REPUBLIKY

Podvod v súvislosti s falošným prevodom peňazí na základe pokynu fiktívneho manažéra je od októbra 2017 evidovaný aj v policajných štatistikách (v tzv. Evidenčno-štatistickom systéme kriminality) v časti Ekonomické trestné činy (Jurisová, 2019). Od tohto času je políciou spracovávaná správa o vývoji trestnej činnosti CEO podvodov, a to jednotlivo za obdobie rokov 2017, 2018, 2019 a ostatná správa za rok 2020. Pred uvedeným obdobím boli údaje spracované v správe za roky 2013 – 2016 (Správa, 2020).

V roku 2020 bolo v Slovenskej republike **zaznamenaných** 39 prípadov CEO podvodov. Za sledované obdobie (týmto obdobím budú pre účel príspevku roky 2017 – 2020), vyplývajúc zo správ spracovaných za tieto roky má početnosť evidovaných CEO podvodov kolísavú tendenciu. V roku 2019 bolo evidovaných o desať viac prípadov ako v roku 2020. V roku 2018 bolo evidovaných dvadsaťsedem prípadov a v roku 2017 bolo evidovaných štyridsaťpäť prípadov.

Z hľadiska **vývinového štádia** trestného činu bolo z celkového evidovaného počtu prípadov spráchaných 10 v štádiu pokusu a v 29 prípadoch išlo o dokonaný trestný čin. V sledovanom odbodí bolo evidovaných viac dokonaných trestných činov ako činov v štádiu pokusu ešte aj v roku 2019. V rokoch 2018 a 2017 bolo evidovaných menej dokonaných trestných činov ako trestných činov v štádiu pokusu. Uvedené môže mať niekoľko vzájomne prelínajúcich sa dôvodov, objektívnych aj subjektívnych, ako napríklad neustále narastajúca odvaha páchateľov, sofistikovanosť trestnej činnosti, nedostatočne účinné kontrolné mechanizmy (tak v podobe prevencie ako aj represie) či medzinárodný aspekt kriminality (Jurisová, 2019(a); Správa, 2017 – 2020).

Pri podvodoch falošných manažérov sú nevyhnutne sledovanými aspektmi – **škoda** ako aj **škodovosť**. Výška škody je evidovaná v dvoch častiach, a to škoda hroziaca a škoda spôsobená. V roku 2020 bola evidovaná spôsobená škoda viac ako 1 milión €, hroziaca škoda presahovala 200 000 €. V roku 2019 bola evidovaná taktiež vyššia suma pri spôsobenej ako pri hroziacej škode, avšak s minimálnym rozdielom – približne 100 000 €, pričom spôsobená aj hroziaca škoda presiahli sumu 1 milión €. V roku 2018 aj v roku 2017 bola evidovaná vyššia suma pri hroziacej ako pri spôsobenej škode, pričom ich hodnoty boli podstatne nižšie v porovnaní s rokmi 2019 a 2020. Celková výška škody samozrejeme súvisí (najmä) s počtom evidovaných prípadov v danom roku. Objektívnejšie je ale posúdenia tzv. škodovosti – t. j. priemernej výšky škody v jednom prípade. V roku 2020 bola zistená škodovosť pri pokuse CEO podvodu približne 20 000 € na jeden prípad a pri dokonanom CEO podvode približne 36 000 € na jeden prípad. Pre porovnanie, že v roku 2020 došlo k zmene – v ostatných rokoch sledovaného obdobia vždy prevyšovala výška hroziacej škody na jeden prípad výšku spôsobenej škody na jeden prípad CEO podvodu. Uvedená situácia v podobe výšky škodovosti bola v ostatnom roku ovplyvnená špecifickými prípadmi, v ktorých išlo o najvyššie škody (Správa, 2020; Jurisová, 2020, Jurisová, 2019).

Príklad z aplikačnej praxe: *V prípade dokonaného CEO podvodu išlo o phishingový útok, v ktorom bola poškodená spoločnosť s ručením obmedzeným, pričom výška škody presahovala 330 000 €. Páchateľ sa v tomto prípade dostal k e-mailovej komunikácii medzi obchodujúcimi spoločnosťami a z falošnej e-mailovej adresy, ktorú zamenil s pôvodnou, zaslal obchodnému referentovi poškodenej spoločnosti prevodný e-mail s informáciou o zmenenom čísle bakového účtu spoločnosti z dôvodu prebiehajúceho auditu, na ktorý požadoval zaslať úhradu plánovanej zálohovej faktúry. Poškodená spoločnosť na základe uvedeného vykonala prevod týchto finančných prostriedkov. Následne bolo zistené, že číslo účtu, na ktorý boli finančné prostriedky zaslané, nie je číslom účtu obchodného partnera tejto spoločnosti.*

*V prípade hroziaceho CEO podvodu išlo o sumu viac ako 47 000 €. Pri tomto pokuse o trestný čin bol využitý spôsob maskovaného e-mailu. Poškodené bolo nemenované mesto (t. j. samospráva). Páchateľ vydávajúci sa za primátora mesta z maskovanej e-mailovej adresy, ktorá sa zobrazovala pod tvarom e-mailovej adresy primátora mesta, kontaktoval zamestnankyňu mesta s otázkou týkajúcou sa zostatku finančných prostriedkov na účte mesta a oznamom, že v daný deň musia zaplatiť požadovanú sumu. Páchateľ v následnej e-mailovej komunikácii zadal zamestnankyni pokyn na úhradu tejto sumy*

*v prospech účtu vedenom v zahraničnej banke. Uvedené sa zamestnankyni mesta nepozdávalo a priamo kontaktovala primátora mesta, pričom pri tejto následnej komunikácii s primátorom mesta bolo zistené, že on žiaden e-mail neposlal a žiadnu úhradu od nej nežiadal.*

Páchatelia požadovali menšie sumy finančných prostriedkov pri týchto podvodných prevodoch ako v predchádzajúcom období. Pravdepodobne s cieľom neupozorňovať, resp. nevzbudzovať pozornosť neobvykle vysokými sumami tak, aby neprekračovali „bežný" rámec výšky obchodných transakcií poškodených subjektov (Správa, 2020).

Jednotlivé **subjekty napadnutné podvodmi fiktívnych manažérov** sú osobitným ukazovateľom pri ich posudzovaní. Poškodenými, resp. objektmi útoku tejto trestnej činnosti, vychádzajúc zo samotnej podstaty CEO podvodov ako konania zameraného na podvodné prevody finančných prostriedkov, čo sa týka dlhodobého vývoja, sú aj naďalej právnické osoby.

V roku 2020 boli najčastejšie napadnutým sujektom právnické osoby – konkrétne obchodné spoločnosti založené fornou s. r. o. (29 objektov útoku) a a. s. (6 poškodených). Uvedené druhy môžeme zaradiť k najzraniteľnejším z dôvodu ľahko verejne prístupných údajov o ich štruktúre v spojitosti s nedostatočným oboznámením zodpovedných osôb s existenciou vyššie uvedeného protiprávneho konania a v nedostatočnom určení štandardných bezpečnostných postupov pri udeľovaní pokynov na akýkoľvek prevod alebo platbu finančnýchh prostriedkov najmä na zahraničné bankové účty pri náhlej požiadavke o úhradu alebo pri náhlej zmene čísla bakového účtu na faktúre. V ostatnom roku boli napadnuté aj tri verejné inštitúcie a jeden živnostník. Nebol napadnutný ani jeden štátny podnik.

K výraznému poklesu útokov došlo pri verejných inštitúciách (v rokoch 2017 – 2019 bolo evidovaných po deväť prípadov). V rokoch 2019 a 2017 boli napadnutnými aj štátne podniky (Správa, 2020).

## 2. FORMY TRESTNEJ ČINNOSTI CEO PODVODOV V PODMIENKACH SLOVENSKEJ REPUBLIKY

V prípade CEO podvodov ide vo všeobecnosti o podvod s platobným príkazom. Je charakteristický sofistikovaným, zosúladeným a vypočítavým útokom. Najmä proti súkromným spoločnostiam, ale aj proti štátnym a verejným organizáciám, v rámci ktorých sú bežne vykonávané elektronické bankové prevody na pokyn nadriadeného (CEO manažéra). Nevyhnutným krokom je prelomenie zabezpečenia e-mailovej komunikácie samotného CEO manažéra, a to za predpokladu, že jeho schránka obsahuje informácie o prebiehajúcich obchodných aktivitách, ale aj o e-mailových adresách jednotlivých zamestnancov. Útočník disponujúci týmito informáciami ich zmanipuluje. Následne sa vydáva za CEO manažéra a osloví subjekt (pracovníka učtárne či samotnú účtovníčku), a to s požiadavkou na prevod finančných prostriedkov do zahraničia. Trestná činnosť v ekonomike (nevynímajúc aj takéto podvody) je páchaná špecifickou skupinou subjektov v diskrétnom prostredí kancelárií. Pre „neodborníka" sú jej odrazy málo výrazné, pretože medzi legálnou a nelegálnou činnosťou v ekonomike sú malé rozdiely.

Je na mieste zamerať pozornosť aj na takzvané **sociálne inžinierstvo** – ako spôsob získavania dôverných informácií pomocou manipulácie. Uvedená metóda bežne využíva internetovú alebo telefónnu komunikáciu, pričom zneužíva dôverčivosť ľudí vydávaním sa za známe a existujúce spoločnosti či inštitúcie. Využitím sociálneho inžinierstva hovoríme o heterogénnych útokoch, od hromadných phishingových e-mailov až po cielené, viacvrstvové a sofistikované útoky s využitím viacerých techník. Avšak všetky majú spoločné to, že sú zamerané na manipuláciu bežných spôsobov ľudského správania sa, pričom existuje iba obmedzená množina technickcýh opatrení na ochranu pred takýmito útokmi (Jurisová, 2019(a); Správa, 2020; Dubeň, 2021).

V roku 2020 **modus operandi** páchateľov CEO podvodov mal formu elektronickej komunikácie – konkrétne maskovaného e-mailu a phishingového útoku. V dvadsiatichsiedmich prípadoch bola využitá forma phishingu (z toho 23 dokonaných prípadov a 4 prípady v štádiu pokusu) a v dvanástich prípadoch forma maskovaného e-mailu (6 dokonaných prípadov a 6 prípadov v štádiu pokusu).

*Phishingový útok* je 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. *Maskovaný e-mail* je 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 manžéra, za ktorého sa páchateľ vydáva.

Rozdiel medzi uvedenými formami je najmä v rozsahu odborných znalostí páchateľa a samotnom technickom prevedení útoku. Vytvorenie maskovanej e-mailovej adresy si vyžaduje v zásade „základné“ počítačové zručnosti alebo využitie návodu relatívne ľahko a rýchlo dohľadateľného v rámci internetu. Následne si páchateľ vytypuje z dostupných zdrojov spoločnosť či orgnaizáciu, ktorá má zverejnené potrebné e-mailové adresy a osloví svoju obeť so žiadosťou o rýchly prevod finančných prostriedkov do zahraničia. Riziko ohrozenia maskovaným e-mailom je v tom, že pred prijímaním podvodných e-mailov sa nedá tak účinne softvérovo brániť. Dokonanie skutku je v takýchto prípadoch často spôsobené zlyhaním ľudského faktora v spojitosti s nedostatočným oboznámením zodpovedných osôb s existenciou vyššie uvedeného protiprávneho konania (v nedostatočnom preventívnom pôsobení CEO manažérov) a v nedostatočnom určení štandardných bezpečnostných (administratívnych) postupov pri udeľovaní pokynov na akýkoľvek prevod alebo platbu finančných prostriedkov najmä na zahraničné bankové účty (dvojitá kontrola, telefonické overovanie pri náhlej požiadavke o úhradu alebo pri náhlej zmene čísla bankového účtu na faktúre a pod.). V prípadoch phishingu je predpoklad, že útočník prenikol do počítača poškodeného subjektu (svojej obete) a disponuje údajmi o jej komunikácii, obchodných aktivitách, vnútornom fungovaní spoločnosti a vo viacerých prípadoch aj údajmi z dostupných sociálnych sietí, ktoré využíva na účel adresného a aj časovo presného koordinovania svojho útoku (neprítomnosť CEO manažéra na pracovisku, zmena čísla účtu na faktúre v už prebiehajúcej obchodnej operácii). Táto metóda zvyšuje úspešnosť samotného CEO podvodu, ale vyžaduje si omnoho väčšie odborné znalosti (cielený sofistikovaný útok). Pri využití tejto metódy býva následne použitá pozmenená faktúra (číslo účtu) v už prebiehajúcom obchode.

V roku 2020 (v porovnaní s rokom 2019) došlo k zvýšeniu prípadov realizovaných využitím metódy phishingu. Dá sa predpokladať, že tento stav je spôsobený tým, že páchatelia disponujú rozsiahlejšími znalosťami v oblasti informačných technológií ako bežní užívatelia, pričom riziko ohrozenia sa zvyšuje aj v dôsledku nedostatočného zabezpečenia komunikácie pri obchodnom styku, neoverovania údajov na faktúrach zo strany poškodených subjektov, postupného zvyšovania využívania služieb elektronického bankovníctva a nárastu transakcií medzi podnikateľskými subjektmi. Páchatelia majú v niektorých prípadoch snahu kontaktovať svoju obeť opakovane, a to až do doby, kedy nedôjde k odhaleniu, že ide o podvod (Správa, 2020).

K jednotlivým prípadom CEO podvodov je vzhľadom na následné konanie páchateľov na mieste uviesť, že ide aj o predikatívny trestný čin k následnej legalizácii výnosu z trestnej činnosti. Výročná správa finančnej spravodajskej jednotky Prezídia Policajného zboru za rok 2019 uvedené potvrdzuje tým, že z *analýzy hlásení neobvyklých obchodných operácií* vyplynulo, že medzi najčastejšie prípady legalizácie výnosov z trestnej činnosti a ich naviazaniu na predikatívnu trestnú činnosť v uvedenom období patrili okrem iných aj podvody – konkrétne CEO podvody.

Príklad z aplikačnej praxe: *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,- € (Výročná, 2019; Jurisová, 2019).*

**„Money mule“** sú významným prvkom realizácie CEO podvodov. Vo väčšine prípadov týchto podvodov potrebuje páchateľ účet v banke, ktorý bude mať pod kontrolou aj napriek tomu, že nebude jeho majiteľom. Na tento účel sú organizovaní rôzni sprostredkovatelia, ktorí či už za úplatu alebo podvodom, riadia účet a následne poskytnú k nemu prístupové práva páchateľom CEO podvodov, alebo na ich pokyn vykonajú príslušné transakcie. Na tento uvedený účel sú využívané práve osoby nazývané money mule. Sú najčastejšie oslovené elektornickou formou, nie zriedka pod zámienkou pracovnej ponuky alebo formou služby za odplatu. V prípade CEO podvodov spáchaných v Slovenskej republike je pravidlom, že finannčné prostriedky sú prevádzané na bankové účty založené v zahraničí, pričom týmto spôsobom sa výrazne zamedzuje možnosti zaistenia finančných prostriedkov a zároveň toto opatrenie slúži k zmareniu identifikácie útočníka, prípadne konečného príjemcu finančných prostriedkov. Vo väčšine prípadov sú tieto finančné prostriedky prevádzané aj niekoľkokrát, kým skončia na bankovom účte, z ktorého sú následne vyberané v hotovosti, a to či už konenčým príjemcom (páchateľom), prípadne ďalšou money mule, ktorá ich odovzdáva páchateľovi alebo následne zasiela páchateľovi (napríklad prostredníctvom využitia služby Western Union). Vo fáze bezhotovostných prevodov dochádza 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, napríklad Čína, Nigéria či Hongkong (Jurisová, 2019(a)).

Pri prevode finančných prostriedkov pochádzajúcich z CEO podvodov v Slovenskej republike sú zisťované údaje o bankových účtoch, na ktoré tieto smerujú. V roku 2020 finančné prostriedky z CEO podvodov smerovali najmä na účty (**pôvod bankového účtu**) vo Veľkej Británii, Turecku, Španielsku či Holandsku. Finannčé prostriedky boli prevedené aj na bankové účty vo Švédsku, Nemecku, Česku, Maďarksu, Poľsku, USA či Číne (Správa, 2020).

## ZÁVER

Vyplývajúc z analýzy údajov zistených v roku 2020 a ich komparáciou s údajmi o trestnej činnosti CEO podvodov v rokoch 2017 – 2019 je možné uvažovať o týchto **záveroch**:

- Znížil sa počet CEO podvodov spáchaných v štádiu pokusu. Počet dokonaných trestných činov bol na rovnakej úrovni ako v roku 2019 – čo naďalej poukazuje na úspešnosť páchateľov a ich metód. Objasniť sa žiaľ nepodarilo ani jeden prípad.
- V roku 2020, najmä v porovnaní s rokom 2019, doško k poklesu výšky škody (spôsobenej aj hroziacej). Zároveň došlo aj k poklesu škodovosti, najmä v prípadoch pokusu o spáchanie CEO podvodu, a to aj v dôsledku poklesu napadnutých (poškodených) subjektov a menších súm požadovaných páchateľmi pri páchaní podvodu.
- Zvýšil sa počet prípadov, pri ktorých páchatelia použili na realizáciu podvodu náročnejší spôsob – phishing – oproti prípadom realizovaným formou maskovaného e-mailu. Uvedené je možné futurologicky ponímať negatívne.
- Pri využití formy phishingu vysoko prevažovali dokonané CEO podvody nad pokusmi. Uvedené poukazuje na úspešnosť tejto sofistikovanejšej a taššie odhaliteľnej formy.
- K najohrozenejším subjektom aj naďalej patria právnické osoby – spoločnosť s ručením obmedzeným a akciová spoločnosť. Zároveň došlo k relatívne výraznému poklesu útokov na verejné inštitúcie.
- Finančné prostriedky pochádzajúce z CEO podvodov realizovaných v Slovenskej republike boli prevedené do zahraničia. Pôvod bankových účtov bol zaznamenaný v najvyššom počte vo Veľkej Británii.

Pozitívom je nepochybne aj monitorovanie prípadov CEO podvodov v Evidenčno-štatistickom systéme kriminality. Na mieste je upriamiť pozornosť aj na to, aby jednotlivé útvary Policajného zboru vykazovali trestnú činnosť CEO podvodov správne, a aby tento špecifický trestný čin nebo evidovaný „iba“ ako „podvod“.

Najčastejšími úkonmi príslušníkov Policajného zboru boli napríklad tieto: previerka e-mailových adries a IP adries počítačov, preverenie čísla bankového účtu, na ktorý boli zaslané finančné prostriedky, vypočutie svedkov či poškodených.

Zvýšenie objasnenosti tejto trestnej činnosti je obmedzené skutočnosťou, že ide o medzinárodný rozmer podvodov, s prvkami ako money mule, zahraničné bankové účty, na ktoré sú prevádzané podvodne vylákané finančné prostriedky, IP adresy počítačov a e-mailové adresy – kde sú závery vyšetrovania závislé od výsledkov medzinárodnej právnej pomoci, ktorá je nepochybne častokrát značne časovo náročná. K hlavným príčinám neobjasňovania týchto prípadov môžeme jednoznačne zaradiť – medzinárodný aspekt a moderné spôsoby zakrývania totožnosti páchateľa prostredníctvom elektronickej komunikácie. Uvedené naznačuje, že lokálne možnosti objasňovania týchto prípadov sú obmedzené, ba až nepostačujúce.

Je predpoklad, že počet prípadov CEO podvodov bude mať klesajúcu tendenciu. Na elimináciu páchania takejto trestnej činnosti je nutné opätovne zvyšovať povedomie občanov osvetou zo strany poskytovateľov platobných služieb, ako aj štátnych orgánov.

Do budúcnosti je predpoklad, že charakter tejto trestnej činnosti bude podobný ako doteraz. Jedným z dôvodov je, že páchatelia dosiahli vysoký stupeň sofistikovanosti pri páchaní CEO podvodov – najmä formou phishingu.

V rámci **prevencie** sa aktuálne javí ako najlepší spôsob ochrany pred CEO podvodmi zvyšovanie bezpečnostného povedomia fyzických a právnických osôb (používateľov e-mailov). Napríklad formou školení, kde sú oboznámení so spôsobom prevedenia útokov pri týchto podvodoch a aj s tým, ako môžu rozpoznať podozrivý e-mail. Taktiež je dobrou praxou mať definované pravidlá nakladania so správami, v ktorých sú požadované vyššie finančné prevody. Predchádzať takýmto podvodom možno iba dôslednou a neustálou kontrolou údajov uvádzaných v dokumentoch v rámci realizácie obchodného vzťahu, ako aj dodatočným overením alebo dvojitým schvaľovaním prevodov finančných prostriedkov v spoločnosti.

Medzinárodný charakter CEO podvodov a potreba preventívneho zacielenia aktivít realizovaných v tejto oblasti sú evidentné. Predmetnej problematike venuje pozornosť aj Europol – napríklad zameriava pozornosť na naznačenie možností/možných reakcií na takýto podvod, tak zo strany obchodnej spoločnosti/organizácie ako aj zo strany zamestnanca.

Tabuľka 1 Možnosti reakcií na CEO podvody zo strany obchodnej spoločnosti/organizácie alebo zamestnanca (Europol, 2019)

| **OBCHODNÁ SPOLOČNOSŤ** | **ZAMESTNANEC** |
|---|---|
| • Dajte si pozor na riziká a zariaďte, aby boli zamestnanci informovaní a opatrní.<br>• Upozornite zamestnancov, aby boli obozretní pri žiadostiach o platbu.<br>• Implementujte interné postupy týkajúce sa platieb.<br>• Implementujte postupy na overenie oprávnenosti žiadostí o platbu prijatých e-mailom.<br>• Nastavte procesy nahlasovania podvodov.<br>• Zvážte, aké informácie uvediete na webovej stránke obchodnej spoločnosti, obmedzte množstvo informácií a buďte opatrní na sociálnych sieťach.<br>• Modernizujte a aktualizujte technické zabezpečenie. | • Prísne dodržujte bezpečnostné postupy pri platbách a nákupe. Nevynechajte žiadne kroky a nepodľahnite tlaku.<br>• Keď pracujete s citlivými informáciami/peňažnými prevodmi, vždy starostlivo skontrolujte e-mailové adresy.<br>• Ak máte pochybnosti o platobnom príkaze, poraďte sa s príslušným pracovníkom.<br>• Nikdy neotvárajte podozrivé odkazy alebo prílohy v e-mailoch. Buďte obzvlášť opatrný, ak si kontrolujete váš súkromný e-mail na pracovnom počítači.<br>• Obmedzte množstvo informácií a buďte opatrný na sociálnych sieťach.<br>• Nezdieľajte informácie o firemnej štruktúre, bezpečnosti a procesoch. |
| **!!! Vždy nahláste polícii pokus o podvod, aj keď ste sa nestali obeťou podvodu**. | **!!! Ak dostanete podozrivý e-mail alebo telefonát, vždy informujte IT oddelenie.** |

Vyplývajúc z doterajších zistení možno predpokladať, že v nastávajúcom období bude vývoj situácie v tejto oblasti do značnej miery ovplyvnený vývojom celosvetovej sitácie v oblasti využívania internetových služieb a nástrojov. Výrazný nárast možno očakávať pri internetových podvodoch, a to z dôvodu zvyšovania záujmu obyvateľstva o internetový spôsob nákupu tovaru, k čomu nepochybne prispieva aj súčasná celospoločenská situácia súvisiaca s ochorením covid-19 (Správa, 2020; Jurisová, 2021).

Poznatky z predmetného príspevku môžu byť využité v bezpečnostnej teórii aj aplikačnej praxi a zároveň v rámci výstupov VVÚ Implementácia zákona o obetiach trestných činov do policajnej a viktimologickej praxe (Výsk. 255), riešenej katedrou kriminológie Akadémie Policajného zboru v Bratislave.

## LITERATÚRA


Čentéš, J. a kol. (2020). Trestný zákon. Veľký komentár 5. aktualizované vydanie. Žilina: Eurokódex. 998 s. ISBN 978-80-8155-066-9.

Dubeň, P. (2021). Príčiny a podmienky kriminality v ekonomike – determinanty odhaľovania a objasňovania trestných činov v ekonomike. In: Odhaľovanie a objasňovanie trestných činov v ekonomike v systéme zabezpečovania neodvratnosti trestného postihu (Zborník vedeckých prác), Bratislava: Akadémia Policajného zboru v Bratislave, s. 79-96. ISBN 978-80-8054-892-6.

EUROPOL. CEO podvod/business email compromise (BEC). [2019-29-9]. Dostupné z: https://www.europol.europa.eu/sites/default/files/documents/sk_0.pdf.

Evidenčno-štatistický systém kriminality.

Hofreiter, L. (2019). O potrebe a význame teórie pre bezpečnostné vzdelávanie. In: Krízový manažment, Žilina: Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, s. 85-94. ISSN 1336.

Jurisová, M. (2019(a)). Vybrané kriminologické aspekty podvodov páchaných prostredníctvom falošných manažérov. In: Policajná teória a prax, r. XXVII, č. 3, s. 87-100. ISSN 1335-1370.

Jurisová, M. (2019). Podvody páchané prostredníctvom falošných manažérov – vybrané aspekty. In: Policajná teória a prax, r. XXVII, č. 4, s. 71-82. ISSN 1335-1370.

Jurisová, M. (2020(a)). Vývoj podvodov páchaných prostredníctvom falošných manažérov v podmienkach Slovenskej republiky. In: Aktuálne otázky trestného práva v teórii a praxi (Zborník príspevkov), Bratislava: Akadémia Policajného zboru v Bratislave, r. 8, s. 71-77. ISBN 978-80-8054-859-9.

Jurisová, M. (2020). Čo sú to CEO podvody? In: Sociálna prevencia, r. 15, č. 1, s. 12-13. ISSN 1336-9679.

Jurisová, M., Nikolajová Kupferschmidtová, E., Comorek, M. (2021). Selected criminological aspects of fraud commerce through false managers. In: Faculty of Security Yearbook. Dostupné z: https://aseestant.ceon.rs/index.php/fb_godisnjak/article/view/29663, No 1, s. 77 – 98.

Marková, V. (2018). Súčasný stav a východiská počítačovej kriminality v právnom poriadku Slovenskej republiky. In: Aktuálne výzvy prevencie počítačovej kriminality, Zborník príspevkov, Bratislava: Akadémia Policajného zboru v Bratislave, s. 106-126. ISBN 978-80-8054-774-5.

Správa o vývoji trestnej činnosti CEO podvodov na území Slovenskej republiky (2020). Úrad kriminálnej polície Prezídia Policajného zboru.

Stieranka, J. 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.

Výročná správa finančnej spravodajskej jednotky (2020). Finančná spravodajská jednotka národnej kriminálnej agentúry Prezídia Policajného zboru Ministerstva vnútra Slovenskej republiky.

Zákon č. 300/2005 Z. z. Trestný zákon.



**Michaela Jurisová, JUDr., PhD.**

Katedra kriminológie, Akadémia Policajného zboru v Bratislave

e-mail: michaela.jurisova@minv.sk; michaela.jurisova@akademiapz.sk